ThinkVantage テクノロジー・デプロイメント・ガイド

以下を含みます。

- Rescue and Recovery バージョン 3.1
- Client Security Solution バージョン 7.00
- 指紋認証ユーティリティー・バージョン 5.5

ThinkVantage

ThinkVantage テクノロジー・デプロイメント・ガイド

第1刷 2006.5

目次

まえがき vii

第 1 章 概要 1

主要なコンポーネント 1
Rescue and Recovery 1
  Rescue and Recovery ワークスペース 2
  Rescue and Recovery (Windows 環境) 3
  Antidote Delivery Manager 3
Client Security Solution 3
  Client Security パスフレーズ 4
  Client Security パスワードの復元 5
  Client Security Password Manager. 5
  SafeGuard PrivateDisk 6
  Security Advisor 7
  証明書転送ウィザード 8
  ハードウェア・パスワードのリセット 8
  TPM のないシステムのサポート. 8
System Migration Assistant 8
ThinkVantage 指紋認証ユーティリティー 9

第 2 章 インストールの注意点 11

Rescue and Recovery 11
  上書きインストールの考慮事項. 11
Client Security Solution. 12
  TPM のソフトウェア・エミュレーション . . . 12
  アップグレードのシナリオ 12

第 3 章 Rescue and Recovery のカスタマイズ 13

基本バックアップへの Sysprep ユーティリティー・イメージの取り込み 13
  複数パーティションを持つ PC の取り込みと、Sysprep イメージ内のファイルを除外. 14
Windows 環境での Rescue and Recovery の使用 . . 16
  レジストリー設定を使用するバックアップ・ファイルの包含と除外 16
  Rescue and Recovery のその他の側面のカスタマイズ. 18
ワークスペース (Predesktop Area) 19
  RRUTIL.EXE の使用 19
  Rescue and Recovery ワークスペースのカスタマイズ. 27
  Opera ブラウザーの設定 33
  画面の解像度の変更 39
  アプリケーションの開始 40
  パスワード 40
  パスワード・アクセス. 41
復元タイプ 42
  ファイルのレスキュー. 42
  個別ファイルの復元 43
  オペレーティング・システムおよびアプリケーション. 43
  システムの活性化 43
  バックアップの完了 44
  全体を復元 44
  工場出荷時/Image Ultra ビルダー 44
パスワードの保存 44
ハードウェア・パスワードのリセット 45
  パッケージ・ビルド 46
  パッケージ・デプロイメント 47
  登録. 47

第 4 章 Client Security Solution のカスタマイズ 49

TPM の使用 49
Client Security Solution の暗号鍵の管理 49
  所有権の取得. 50
  ユーザー登録. 51
  ソフトウェア・エミュレーション 52
  システム・ボードの交換 52
XML スキーマの使用 54
  使用法 54
  例 55

第 5 章 System Migration Assistant のカスタマイズ 65

コマンド・ファイルの作成 65
ファイル・コマンド 66
ファイル移行コマンド. 69
ファイル移行コマンドの例 72
  取り込みフェーズでのファイルの選択 72
追加アプリケーション設定の移行 74
  アプリケーション・ファイルの作成 79
  Adobe Reader 用の application.xml ファイルの例 81

第 6 章 インストール 87

Rescue and Recovery および Client Security Solution のインストール 87
  インストール要件 87
  インストール・コンポーネント 89
  ログ・ファイルのインストール. 92
  インストールするソフトウェアのシナリオ . . . 93
  ソフトウェアの状態変更 94
  Rescue and Recovery のインストール. 97
  Client Security Solution のインストール. . . . 102
指紋認証ユーティリティーのインストール. . . . 104
  サイレント・インストール 104
  System Management Server (SMS) のインストール 105
  オプション 105

第 7 章 Antidote Delivery Manager のインフラストラクチャー 107
リポジトリー 107
Antidote Delivery Manager および Windows コマンド 108
Antidote Delivery Manager の使用方法 109
大規模なワームの攻撃 109
小規模なアプリケーション更新 110
VPN およびワイヤレス・セキュリティーの対応 111
Virtualization Module for Antidote Delivery Manager 111
要件 111
インストール 112
概要 113

第 8 章 指紋認証ユーティリティー . . 117
ユーザー固有コマンド 117
グローバル設定のコマンド 118
保護モードおよび簡易モード 119
保護モード - 管理者 120
保護モード - 制限ユーザー. 120
簡易モード - 管理者 121
簡易モード - 制限ユーザー. 122
ThinkVantage 指紋認証ユーティリティーおよび Novell Netware Client. 122

第 9 章 ベスト・プラクティス 125
Rescue and Recovery および Client Security Solution のインストールのデプロイメント例 125
デプロイメント・シナリオ 1 125
デプロイメント・シナリオ 2 129
デプロイメント・シナリオ 3 131
デプロイメント・シナリオ 4 135
デプロイメント・シナリオ 5 138
デプロイメント・シナリオ 6 138
Sysprep のバックアップ/復元 139
Client Security Solution モードの切り替え . . . 139
Computrace と Rescue and Recovery 140
企業用 Active Directory のロールアウト . . . 140
CD またはスクリプト・ファイルのスタンドアロン・インストール 140
システムの更新. 140
System Migration Assistant 140

付録 A. インストール・コマンド・ライン・パラメーター 141
管理用インストールの手順およびコマンド・ライン・パラメーター 141
msiexec.exe の使用. 141

付録 B. Rescue and Recovery のカスタマイズ. 145
バックアップおよび関連タスクのスケジューリング 145
バックアップ用ネットワーク・ドライブの割り当て 145
ネットワーク・バックアップ用のユーザー・アカウントのセットアップ 146

付録 C. コマンド・ライン・ツール. . . 147
Antidote Delivery Manager 147
Mailman 147
Antidote ウィザード 147
パスワードの設定 147
Client Security Solution 147
SafeGuard PrivateDisk 147
Security Advisor. 149
Client Security Solution セットアップ・ウィザード 150
デプロイメント・ファイルの暗号化または暗号化解除ツール 151
デプロイメント・ファイル処理ツール 152
TPMENABLE.EXE 152
Active Directory のサポート 153
管理用 (ADM) テンプレート・ファイル . . . 153
グループ・ポリシーの設定 154
eGatherer 188
MAPDRV. 188
Rescue and Recovery ブート・マネージャーの制御 (BMGR32) 190
RELOADSCHED 194
RRCMD コマンド・ライン・インターフェース 194
System Migration Assistant 197
System Update 197

付録 D. 管理者ツール 199
Antidote ウィザード 199
BMGR CLEAN 199
CLEANDRV.EXE 200
CONVDATE 200
CREAT SP 201
RRUTIL.EXE 202
SP.PQI. 202

付録 E. ユーザーの作業 203
Windows XP. 203
Windows 2000 204
レスキュー・メディアの作成 205

付録 F. Antidote Delivery Manager コマンドの解説および例 207
Antidote Delivery Manager コマンドのガイド . . . 207
サポートされる Microsoft コマンド 211
準備およびインストール. 212
準備 212
設定 212
リポジトリー 212
スケジュール情報 212
署名キー 213
ネットワーク・ドライブ. 213
クライアント PC でのインストール 214
サーバー・インフラストラクチャー 214
単純なシステムのテスト - 通知の表示 214
デプロイメント. 214
例 217

スクリプトの例. 219

付録 G. 特記事項 221

商標 222

用語集 223

まえがき

本書に記載されている情報は、ThinkVantage™ プログラムをサポートし、Lenovo™ Care をサポートしていません。Lenovo Care について詳しくは、Lenovo Web サイト http://www.ibm.com/jp/pc/innovation/lenovocare/ を参照してください。

本書は、IT 管理者、または Rescue and Recovery™ プログラムを組織内の PC にデプロイする担当者を対象としています。Rescue and Recovery は、スマートセンターへの電話サポート要請や修理依頼などをせずに、お客様の業務をより効率的に進めていただくためのツールです。Rescue and Recovery は、Microsoft® Windows® オペレーティング・システムが立ち上がらない、あるいは正しく稼働しない場合に、ユーザーおよび管理者がバックアップからの復元、ファイルへのアクセス、問題の診断、およびイーサネット接続を行うことができるツールです。また、破壊されたかまたはネットワーク上にないシステムへのクリティカルな更新のデプロイメントを可能にし、復元の実行時に自動的にシステムへパッチを適用します。本書は、Rescue and Recovery アプリケーションを 1 台以上の PC にインストールするために必要な情報を提供します。各ターゲット PC で同ソフトウェアのライセンスが有効であることが条件となります。また、IT または企業方針をサポートするためにカスタマイズすることができるツールの多くの特徴についての情報を提供しています。

Rescue and Recovery は、機能およびアプリケーション・ヘルプを提供します。Rescue and Recovery ワークスペースに組み込まれているさまざまなコンポーネントの使用に関する質問および情報は、そのコンポーネントのオンライン・ヘルプ・システム (http://www.ibm.com/jp/pc/think/thinkvantagetech/) を参照してください。

このデプロイメント・ガイドは、IT プロフェッショナルおよび固有の目標を念頭に作成されています。ご提案またはコメントは、Lenovo 認定担当者にご連絡ください。本書は定期的に更新されるため、次の Web サイトで将来の資料を確認してください。

http://www.ibm.com/jp/pc/think/thinkvantagetech/

第 1 章 概要

本章では、このデプロイメント・ガイドに記載されているプログラムの概要を示します。本デプロイメント・ガイドで説明されているテクノロジーは、PC の使い勝手と自己完結性を向上させ、ロールアウトを促進し単純化する強力なツールを提供するので、IT プロフェッショナルには大きなメリットをもたらします。
ThinkVantage® テクノロジーの支援により、IT プロフェッショナルは、個別の PC の問題を解決する時間を短縮できるので、中核となる作業に多くの時間を費やすことができるようになります。

主要なコンポーネント

本書の主要なコンポーネントは、以下のとおりです。

- ThinkVantage Rescue and Recovery
- ThinkVantage Client Security Solution
- ThinkVantage System Migration Assistant
- ThinkVantage 指紋認証ユーティリティー

注: 本デプロイメント・ガイド全体を通して、Lenovo は、管理者がインストールおよびカスタマイズの機能を実行する上で役立つコマンド・スクリプトを提供しています。これらのコマンド・スクリプトは、対応するページに収まるように変更されました。これらのコマンド・スクリプトを 1 つの文字列コマンドとして入力してください。

Rescue and Recovery

Rescue and Recovery は、ThinkVantage テクノロジー製品のうちの 1 製品です。このアプリケーションは、Microsoft Windows オペレーティング・システムが起動しない場合であっても使用できるツール群から構成されています。

Rescue and Recovery には、以下の機能があります。

- Windows オペレーティング・システムとは独立させて起動することができる Rescue and Recovery ワークスペース。
- Rescue and Recovery (Windows 環境): ファイルのバックアップ、ファイルのレスキュー、およびオペレーティング・システムおよびファイルのリカバリーをすることができます。
- Antidote Delivery Manager

注: Rescue and Recovery には、Windows オペレーティング・システムで実行される機能があり、Windows の実行中に Rescue and Recovery ワークスペースで使用されるシステム情報なども収集されます。Windows オペレーティング・システムが誤動作しても、 Rescue and Recovery ワークスペースの正常な動作が妨げられることはありません。ただし、Windows オペレーティング・システムで実行される機能について、本デプロイメント・ガイドでは説明しません。

Rescue and Recovery ワークスペース

Rescue and Recovery ワークスペースは、ユーザーの PC で Windows を起動できない場合の緊急用の作業環境です。この環境は、Windows のような外観および機能を提供し、ユーザーは IT スタッフの時間を取らずに問題を自己解決できます。

Rescue and Recovery ワークスペースには、以下の 4 つの主要カテゴリーの機能があります。

- **レスキューおよび復元**
  - **復元の概要:** さまざまなリカバリー・オプションに関するヘルプ・トピックへのリンクを提供します。
  - **ファイルのレスキュー:** Windows 上に保存されているファイルを外部メディアまたはネットワーク上の共有フォルダーにコピーし、使用不可のワークステーションとも一緒に作業を続けられます。
  - **システムの復元:** Rescue and Recovery でバックアップしたファイルを復元します。
- **構成**
  - **構成の概要:** 設定に関する Rescue and Recovery ワークスペースのヘルプ・トピックを提供します。
  - **パスワード/パスフレーズの復元:** ユーザーまたは管理者が、Rescue and Recovery 環境でパスワードまたはパスフレーズをリカバリーできるようにします。
  - **BIOS へのアクセス:** BIOS Setup Utility プログラムを開きます。
- **通信**
  - **通信の概要:** 関連する Rescue and Recovery ワークスペースのヘルプ・トピックを提供します。
  - **ブラウザーを開く:** Opera Web ブラウザーを起動します (Web またはイントラネットにアクセスするには、有線イーサネットによる接続が必要です)。
  - **ファイルのダウンロード:** 必要なファイルを ¥SWSHARE フォルダーにある Windows(R) 区画にダウンロードできます。
  - **ネットワーク・ドライブの割り当て:** ソフトウェアのダウンロードやファイルのレスキューを行うためにネットワーク・ドライブを割り当てます。
- **トラブルシューティング**
  - **診断の概要:** Rescue and Recovery 診断ヘルプ・トピックを提供します。
  - **ハードウェアの診断:** PC-Doctor を起動し、ハードウェア・テストを実行後、結果を報告します。
  - **診断ディスクの作成:** 一連の診断ディスケットを作成できます。
  - **別のデバイスから起動:** Rescue and Recovery CD、バックアップ CD セット、内蔵ドライブ、または取り外し可能ストレージ・デバイス (USB ハードディスク・ドライブなど) から起動できます。
  - **システム情報:** PC およびそのハードウェア・コンポーネントに関する詳細情報を表示します。
  - **イベント・ビューアー:** 問題判別および解決を補助するために、 PC へのアクセス状況や PC ハードウェアのリストの詳細を提供します。このログ・ビューアーにより、イベント・ビューアーの項目が読みやすく表示されます。
  - **保証状況**

Rescue and Recovery は、プリインストールされている Lenovo 製 PC で使用できます。

145 ページの『付録 B. Rescue and Recovery のカスタマイズ』に、 Rescue and Recovery 環境をデプロイメント用に設定する方法が記載されています。

注: 最後の Windows 管理者 ID が、Windows から Rescue and Recovery ワークスペースに自動的に繰り上げられる唯一の ID です。Windows の制限ユーザーおよびパワー・ユーザーは、Rescue and Recovery ワークスペースにログオンするために自分のユーザー ID およびパスワードを再入力する必要があります。

Rescue and Recovery (Windows 環境)

Rescue and Recovery (Windows 環境) では、Windows オペレーティング・システムが起動しなくなってもボタンを押すだけで、失われたデータ、アプリケーション、およびオペレーティング・システムのレスキューを行うことができます。この機能により、ヘルプ・デスクへの問い合わせが減り、結果としてサポート・コストを節約できます。

また、バックアップをスケジュールすることができるので、リスクを軽減し、ダウン時間を短縮することが可能です。Rescue and Recovery は、サーバーまたは外部ストレージへの自動外部バックアップを事前設定することにより、さらなるサポートを提供することができます。

バックアップは、デフォルトで 256 AES 鍵により暗号化されます。 Client Security Solution バージョン 7.0 をインストールする場合は、ハードウェアまたはハードウェア・エミュレーションによって保護されるソフトウェア・キーを使用して暗号化することができます。

Antidote Delivery Manager

Antidote Delivery Manager は、ThinkVantage Rescue and Recovery に組み込まれたアンチウィルス、アンチワーム・インフラストラクチャーです。その目的は、素早く実行でき、管理者が問題の報告から数分間のうちに遮断および回復作業を開始できることです。 Antidote Delivery Manager は、1 人の管理者によって起動でき、ネットワークに接続されていないシステムでも機能します。Antidote Delivery Manager は既存のアンチウィルス・ツールに置き換わるものではなく、それを補完するもので、ウィルス・スキャン・ツールの保守や、パッチの取得は引き続き必要です。 Antidote Delivery Manager は、破壊的活動を停止し、パッチを当てるためのインフラストラクチャーを提供します。

Client Security Solution

Client Security Solution ソフトウェアの第一の目的は、お客様が資産としての PC を保護し、PC 上の機密データを保護し、さらに PC がアクセスするネットワーク接続を保護することを補助することです。 (TCG (Trusted Computing Group) という業界団体が仕様を定めている TPM (Trusted Platform Module) を含む Lenovo システムの場合、Client Security Solution ソフトウェアは、システムのトラステッド・ルートとしてハードウェアを活用します。システムにエンベデッド・セキュリティー・チップが含まれていない場合、Client Security Solution は、システムのトラステッド・ルートとしてソフトウェア・ベースの暗号化鍵を活用します。)

Client Security Solution バージョン 7.0 には、以下の機能が含まれています。

- **セキュアなユーザー認証**

  ハードウェアで保護された Client Security パスフレーズが必要です。ユーザーは、このパスフレーズを使用して Client Security Solution で保護された機能にアクセスします。

- **指紋によるユーザー認証**

  内蔵、または USB 接続の指紋センサーを活用し、パスワードで保護されたアプリケーションに対してユーザーを認証します。

- **多層のユーザー認証による Windows ログオンおよびさまざまな Client Security Solution 操作**

  さまざまなセキュリティー関連操作に対して複数の認証装置 (Windows パスワード/Client Security パスフレーズおよび指紋) を定義します。

- **保護**

  ハードディスク上のセキュアな場所に保管することにより、機密ファイルを暗号化します。この場合は、有効なユーザー認証、適切に構成されたセキュリティー・チップ、またはソフトウェア・エミュレーション・チップが必要になります。

- **ログオン・パスワードの管理**

  ユーザー ID やパスワードなどの重要なログオン情報を安全に管理し、保管します。

- **パスワード/パスフレーズの復元**

  ユーザーが Windows パスワードを忘れた場合に、事前構成された質問に答えることで、Client Security パスフレーズを使用して自分で復元できるようにします。

- **セキュリティー設定の監査**

  ユーザーが、詳細なワークステーション・セキュリティー設定のリストを表示し、定義された規格に準拠するように変更できるようにします。

- **ディジタル証明書の転送**

  ハードウェアは、ユーザーと PC の証明書の秘密鍵を保護します。

Client Security パスフレーズ

Client Security パスフレーズは、Client Security Solution アプリケーションに拡張セキュリティーを提供する、ユーザー認証の追加フォームです。 Client Security パスフレーズの要件は、以下のとおりです。

- 8 文字以上の長さ
- 数字が 1 文字以上入っていること
- 最近の 3 回のパスフレーズと異なること
- 反復文字は 2 文字以内
- 先頭に数字を使用しない
- 末尾に数字を使用しない

- ユーザー ID を含めない
- 現在のパスフレーズを設定してから 3 日以内は変更しない
- 現在のパスフレーズと同一の文字を連続して 3 文字以上使用しない
- Windows パスワードと異なる

Client Security パスフレーズを知っているのは個々のユーザーだけであり、 Client Security パスフレーズを忘れた場合に復元する唯一の方法は、 Client Security パスワード復元機能の活用です。ユーザーが復元のための質問に対する回答を忘れてしまった場合、 Client Security パスフレーズで保護されたデータをリカバリーする方法はありません。

Client Security パスワードの復元

このオプションの設定を使用すると、登録された Client Security ユーザーは、Windows パスワードや Client Security パスフレーズを忘れた場合に、3 つの質問に正しく答えることにより、復元することができます。この機能が使用可能である場合、Client Security ユーザーの登録中に、各ユーザーは、10 の質問の中から 3 つを選択し、それぞれの質問に対する回答を入力します。ユーザーがこれまでに自分の Windows パスワードや Client Security パスフレーズを忘れたことがある場合は、これら 3 つの質問に回答して、そのパスワードやパスフレーズを自分でリセットするというオプションが用意されています。

注:

1. Client Security パスフレーズを使用する場合、Client Security パスワードの復元機能は忘れたパスフレーズを復元するための唯一のオプションです。ユーザーは、それら 3 つの質問に対する回答を忘れた場合、登録ウィザードを再実行しなくてはならず、前の Client Security 保護データはすべて失われます。
2. Client Security を使用して Rescue and Recovery ワークスペースを保護する場合、「パスワード復元」によって、ユーザーの Client Security パスフレーズおよび/または Windows パスワードが実際に示されます。パスフレーズまたはパスワードが表示されるのは、Rescue and Recovery ワークスペースが Windows パスワードの変更を自動的に実行する機能を持たないためです。ワイヤレス (ネットワークに接続されていないローカル・キャッシュ・ドメイン) ユーザーが Windows ログオンでこの機能を実行する場合にも、パスフレーズまたはパスワードが表示されます。

Client Security Password Manager

Client Security Password Manager を使用すると、ユーザー ID、パスワード、およびその他の個人情報などの、忘れやすいアプリケーションや Web サイトのログイン情報を管理することができます。 Client Security Password Manager は、ユーザーのアプリケーションや Web サイトへのアクセス全体がセキュアに保たれるように、エンベデッド・セキュリティー・チップを介して情報を保管します。また、Client Security Password Manager プログラムでは、1 つのパスワードまたはパスフレーズを覚えておくか、指紋を使用すればよいため、時間と労力が節約されます。

Client Security Password Manager を使用すると、以下の機能を実行できます。

- **エンベデッド・セキュリティー・チップによるすべての保管情報の暗号化**

  エンベデッド・セキュリティー・チップを介してすべての情報を自動的に暗号化します。これにより、重要なパスワード情報が、Client Security Solution 暗号化鍵によって保護されます。
- **ユーザー ID とパスワードの自動入力**

  ログオン情報がすでに Client Security Password Manager に入力されているアプリケーションや Web サイトにアクセスする際に、ログイン情報を自動的に入力して、ログイン・プロセスを自動化します。
- **Client Security Password Manager インターフェースを使用した項目の編集**

  アカウント項目を編集し、すべてのオプションのパスワード機能を 1 つの使いやすいインターフェースにセットアップすることができます。このインターフェースにより、パスワードと個人情報の管理を迅速かつ容易に行えるようになります。
- **Windows デスクトップのアイコン・トレイから、または単純なキーボード・ショートカットを使用したログオン情報へのアクセス**

  別のアプリケーションや Web サイトを Client Security Password Manager に追加する必要があるときに、容易にログオン情報へアクセスできるようになります。Client Security Password Manager の各機能にも、単純なキーボード・ショートカットによって容易にアクセスできます。
- **ログイン情報のエクスポートとインポート**

  重要なログイン情報をエクスポートして、その情報を PC 間で安全に移動させることができます。 Client Security Password Manager からログイン情報をエクスポートすると、パスワードで保護されたエクスポート・ファイルが作成されます。このファイルは、取り外し可能メディアに保管することができます。このファイルを使用して、あらゆる場所でユーザー情報とパスワードにアクセスしたり、Password Manager を使用して項目を別の PC にインポートします。

  注:

  – インポートが機能するのは Client Security Solution バージョン 7.0 のみです。Client Security Software バージョン 5.4X 以前のバージョンは、 Client Security Solution バージョン 7.0 Password Manager にインポートされません。

SafeGuard PrivateDisk

SafeGuard PrivateDisk を使用して、PC に保管されている機密データを保護します。その機能は、PC、すべてのディスク・ドライブおよび取り外し可能メディア上にある重要な機密情報を保護する電子金庫のようなものです。認証されない人物が保護情報にアクセスしたり、読み取ったりすることはできません。

SafeGuard PrivateDisk は、仮想ディスクの原理に基づいており、暗号化された仮想ディスク・ドライブを作成します。この暗号化された仮想ディスクは、追加のハードディスクのように見えますが、ボリューム・ファイルというファイルです。ボリ

ューム・ファイルは、PC 全体の内容を安全に保管し、最新の高速アルゴリズムを使用して暗号化されます。次のリストに、SafeGuard PrivateDisk に組み込まれた機能の例を示します。

- 仮想ディスクは、次のように使用可能なあらゆるドライブ上に作成することができます。
  - 取り外し可能メディア (ディスケット、USB 取り外し可能ドライブ、CD-ROM、DVD、または Zip ドライブなど)
  - ハードディスク
  - ネットワーク・ドライブ
- ドライバーは、ハードディスクのように機能し、以下のタスクを実行します。
  - オペレーティング・システムは、書き込みおよび読み取りコマンドをドライバーに透過的に送信します。
  - ドライバーは、暗号化されたストレージを管理します。
  - データとディレクトリー情報は、すべて暗号化されます。
- SafeGuard PrivateDisk は、Client Security Solution および TPM とともに機能し、SafeGuard PrivateDisk で生成されたディジタル証明書を保護します。
- SafeGuard PrivateDisk は、以下の対称暗号アルゴリズムと各仮想ディスク用の新しいランダム AES 鍵を併用します。
  - AES、128 ビット、暗号化ブロック・チェーン
  - 各仮想ディスク用の新しいランダム鍵
- 認証は、以下を介して行われます。
  - パスワード
  - 秘密鍵 (X.509 証明書)、オプションのスマート・カード
  - 自動生成された暗号化ファイル・システム証明書を使用できます
- パスワード・セキュリティーは、以下のとおりです。
  - 公開鍵暗号方式ステートメント #5 (PKCS#5)
  - 不正なパスワードの提示による時刻の遅延
  - インターセプト保護を表示するパスワード・ダイアログ

Security Advisor

Security Advisor ツールを使用すると、現在 PC に設定されているセキュリティー設定の要約を表示できます。これらの設定値を使用して、現在のセキュリティー状況を表示したり、システム・セキュリティーを強化することができます。表示されるカテゴリーのデフォルト値は、Windows レジストリーによって変更できます。以下に、いくつかのセキュリティー・カテゴリーを示します。

- ハードウェア・パスワード
- Windows ユーザー・パスワード
- Windows パスワード・ポリシー
- 保護スクリーン・セーバー
- ファイル共有

証明書転送ウィザード

Client Security の証明書転送ウィザードは、ソフトウェア・ベースの Microsoft® 暗号サービス・プロバイダーからハードウェア・ベースの Client Security Solution CSP に、証明書に関連した秘密鍵を転送するすべてのプロセスをガイドします。転送が行われた後は、秘密鍵がエンベデッド・セキュリティー・チップによって保護されるため、証明書を使用する操作はよりセキュアになります。

ハードウェア・パスワードのリセット

このツールは、Windows とは独立して稼動するセキュアな環境を作成し、忘れてしまったパワーオン・パスワードやハードディスク・パスワードをリセットする際に役立ちます。 ID は、自分で作成した一連の質問に回答することによって設定されます。パスワードを忘れる前に、このセキュアな環境をできるだけ早く作成してください。登録後、ハードディスク上にこのセキュアな環境を作成するまでは、忘れてしまったハードウェア・パスワードをリセットすることはできません。このツールは、一部の PC を選択した場合のみ、使用可能です。

TPM のないシステムのサポート

Client Security Solution バージョン 7.0 は現在、対応するエンベデッド・セキュリティー・チップのない IBM および Lenovo システムをサポートしています。このサポートにより、一貫したセキュアな環境を作成するために、全社的な標準インストールを行うことが可能になります。組み込みセキュリティー・ハードウェアを持つシステムは、アタックに対して、より堅固ですが、追加のセキュリティーと機能性もソフトウェア専用 PC にとって有益です。

System Migration Assistant

System Migration Assistant は、システム管理者がユーザーの作業環境を、あるシステムから別のシステムに移行する場合に使用できるソフトウェア・ツールです。ユーザーの作業環境には、以下のものがあります。

- オペレーティング・システム設定 (たとえば、デスクトップおよびネットワーク接続設定)。
- ファイルとフォルダー。
- カスタマイズされたアプリケーション設定 (たとえば、Web ブラウザーのブックマーク、Microsoft Word の編集設定)。
- ユーザー・アカウント。

システム管理者は System Migration Assistant を使用して、企業の標準作業環境をセットアップしたり、個々のユーザーの PC をアップグレードしたりできます。個々のユーザーは System Migration Assistant を使用して、PC をバックアップしたり、設定とファイルを 1 つの PC システムから別の PC システムに移行したりできます。たとえば、デスクトップ PC からモバイル PC (ノートブック PC) に移行することができます。

ThinkVantage 指紋認証ユーティリティー

Lenovo が提案する指紋センサーの目的は、パスワードの管理に関連したコストの削減やシステムに対するセキュリティーの強化においてお客様を補助し、お客様が規制に対応できるようにすることです。 Lenovo 社の指紋センサーとともに、ThinkVantage 指紋認証ユーティリティーを使用すると、個々の PC およびネットワークでの指紋認証が可能になります。Client Security Solution バージョン 7.0 と結合された ThinkVantage 指紋認証ユーティリティーは、拡張機能を提供します。以下のサイトには Lenovo 指紋センサーについての詳細があり、ソフトウェアをダウンロードすることができます。

http://www.ibm.com/jp/pc/think/thinkvantagedesign/fprint.shtml

ThinkVantage 指紋認証ユーティリティーは、以下の機能を提供します。

- **Client Security Software の機能**
  - **Microsoft Windows パスワードの置換:**

    パスワードをお客様の指紋に置き換えて、容易で高速、かつ安全なシステム・アクセスを提供します。
  - **BIOS パスワード (パワーオン・パスワードとも呼ばれます) およびハードディスク・パスワードの置換:**

    これらのパスワードをお客様の指紋と置き換えて、ログオン・セキュリティーと利便性を高めます。
  - **BIOS および Windows へのシングル・スワイプ・アクセス:**

    始動時に指紋をセンサーに読み込ませるだけで、BIOS と Windows にアクセスすることができるので、貴重な時間を節約することができます。
  - **Client Security Solution との統合:** Client Security Solution Password Manager と併用して、TPM を活用します。ユーザーは、指紋センサーに読み込ませて Web サイトにアクセスし、アプリケーションを選択します。
- **管理者機能**
  - **セキュリティー・モードの切り替え:**

    管理者は、セキュア・モードと便利モードを切り替えて、制限ユーザーのアクセス権限を変更することができます。
  - **管理コンソール:**

    スクリプト駆動コマンド・ライン・インターフェースにより指紋認証ユーティリティーのリモート・ソフトウェアのカスタマイズを可能にして、管理者を補助します。
- **セキュリティー機能**
  - **ソフトウェア・セキュリティー:**

    システムに保管する際や、読み取り装置からソフトウェアに転送する際に、強い暗号化により、ユーザー・テンプレートを保護します。

– **ハードウェア・セキュリティー:**

セキュリティー読み取り装置には、指紋テンプレート、BIOS パスワード、および暗号鍵を保管し保護するコプロセッサーがあります。

第 2 章 インストールの注意点

ThinkVantage Rescue and Recovery または Client Security Solution をインストールする前に、インストールするアプリケーションのアーキテクチャーを理解する必要があります。本章では、各アプリケーションのアーキテクチャー、およびすべてのプログラムをインストールする前に必要な追加情報について説明します。

Rescue and Recovery

Rescue and Recovery には 2 つの主要なインターフェースがあります。 1 つめのインターフェースは Windows XP または Windows 2000 環境で作動します。 2 つめのインターフェースは、Rescue and Recovery ワークスペース環境で、Windows XP または Windows 2000 オペレーティング・システムのいずれとも独立して作動します。

注:

1. Rescue and Recovery が最初にインストールされて、次に Computrace がインストールされた場合、Rescue and Recovery は Computrace の非 BIOS バージョンとのみ連動します。 125 ページの『第 9 章 ベスト・プラクティス』 を参照してください。
2. 仮想パーティションとしてインストール済みの Rescue and Recovery ワークスペースでインストールされた Rescue and Recovery を使用する PC 上でストレージ管理サブシステムのインストールを試みた場合、ストレージ管理サブシステムはインストールしません。 Rescue and Recovery ワークスペースとストレージ管理サブシステムは両方とも自身のファイル・システムに C:¥minint フォルダーを使用します。同時に両方をインストールする方法は、タイプ 12 区画として Rescue and Recovery 3.1 をインストールすることです。説明は、 138 ページの『デプロイメント・シナリオ 5』を参照してください。
3. 考えられるセキュリティー・リスクは、Microsoft 回復コンソールが Rescue and Recovery を持つシステム上でインストールされるときに起こります。Microsoft 回復コンソールは、パス C:¥*¥system32¥config¥ ですべてのフォルダーを検索し、このパスが検出された場合はそれがオペレーティング・システムであると仮定します。 Windows パスワードを要求するレジストリー項目がない場合、回復コンソールはユーザーにオペレーティング・システムの選択を許可し、パスワードを入力せずにハードディスク全体へアクセスできるようにします。

上書きインストールの考慮事項

以前のバージョンの古いバックアップはインストール中に削除されるため、Rescue and Recovery 3.1 のインストール後、新規でバックアップを取り直す必要があります。このバックアップは、スクリプトまたはユーザー・インターフェースを使用して行うことができます。

注: 以前のバージョンの Rescue and Recovery 1.0、2.0、および 3.0 から取り込まれたバックアップ・ファイルは、Rescue and Recovery バージョン 3.1 でリカバリーすることはできません。

Client Security Solution

Client Security Solution バージョン 7.0 は必要なドライバーとソフトウェア・サポートを含み、Client Security Solution 7.0 を受信する PC のセキュリティー・ハードウェア (TPM) を使用可能にします。TPM は、エンベデッド・セキュリティー・チップです。チップは実際には BIOS を介して制御され、手順を完了するために正常な BIOS 認証を必要とするので、ハードウェアを使用可能にするには少なくとも 1 回再起動することが必要です。 BIOS 管理者またはスーパーバイザー・パスワードが設定されている場合は、TPM を使用不可にしてから、再び使用可能にする必要があります。

TPM によっていずれかの機能が実施される前に、最初に所有権を初期化する必要があります。各システムは、Client Security Solution オプションを制御する 1 人の Client Security Solution 管理者を持ちます。この管理者は、Windows 管理者特権を持っている必要があります。管理者は XML デプロイメント・スクリプトを使用して初期化することができます。

システムの所有権が構成されたあとは、このシステムにログインする追加の各 Windows ユーザーは、ユーザーのセキュリティー・キーおよびクレデンシャルを登録し初期化するために、Client Security セットアップ・ウィザードによって自動的にプロンプトが出されます。

TPM のソフトウェア・エミュレーション

Client Security Solution は、限定されたシステム上で TPM を使用せずに実行するオプションを持っています。この機能は、ハードウェア保護キーを使用する代わりにソフトウェア・ベースのキーを使用する以外は同じです。ソフトウェアは、TPM に効力を与える代わりに、常にソフトウェア・ベースのキーを使用するように強制するスイッチでインストールすることが可能です。このスイッチを使用するかどうかはインストール時の決定で、ソフトウェアのアンインストールおよび再インストールをすることなしに戻すことはできません。

TPM のソフトウェア・エミュレーションを強制する構文は以下の通りです。

```
InstallFile.exe "/v EMULATIONMODE=1"
```

アップグレードのシナリオ

Client Security Solution の前のレベルからのアップグレードについての詳細は、93 ページの『インストールするソフトウェアのシナリオ』を参照してください。

第 3 章 Rescue and Recovery のカスタマイズ

Rescue and Recovery をインストールする前に、Rescue and Recovery で選択可能なカスタマイズについて理解する必要があります。この章では、ThinkVantage Rescue and Recovery をカスタマイズするために使用する情報を提供しています。以前は、Rescue and Recovery は tvt.txt ファイルを使用してカスタマイズされていました。Lenovo はカスタマイズの手法を更新したため、カスタマイズはレジストリーおよび rnrdeploy.xml ファイルを使用して行われます。デフォルトの rnrdeploy.xml ファイルがカスタマイズされてインストールされると、Rescue and Recovery の設定および Client Security Solution はレジストリーを使用して管理されます。デフォルトの rnrdeploy.xml ファイルは、
http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN でダウンロードすることができます。

Lenovo は、rnrdeploy.xml ファイルの設定ごとに値と説明が記載された本デプロイメント・ガイドの補足資料を作成しています。この補足資料には、rnrdeploy.xml ファイルおよび Active Directory によって使用される設定の両方に関する情報が記載されています。この補足資料は、Lenovo Web サイト
(http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-RNRCDG) からダウンロードできます。

Active Directory について詳しくは、153 ページの『Active Directory のサポート』を参照してください。

基本バックアップへの Sysprep ユーティリティー・イメージの取り込み

基本バックアップに Sysprep イメージを取り込むには、次のようにします。

1. 管理用インストールを実行します。

```
:: Extract the WWW EXE to the directory C:¥TVTRR
start /WAIT setup_tvtrnr_xxxx.exe /a /s /v"/qn TARGETDIR
(where XXXX is the build ID)
="C:¥TVTRR" REBOOT="R"" /w
```

2. MSIEXE ファイルを使用して Rescue and Recovery をインストールするには:
   a. すべての MSI ファイルで次のインストール・ログ生成コードを追加します。

   ```
   /L*v %temp%¥rrinstall.txt
   ```

   b. MSIEXE ファイルを使用してインストールするには、次のコマンドを実行します。

   ```
   : Perform the install of Rescue and Recovery

    msiexec /i "C:¥TVTRR¥Rescue and Recovery.msi"
   ```

   c. MSIEXE を使用してサイレント・インストールするには:

   最後に起動をする場合は、次のコマンドを実行します。

```
: Silent install using the MSI with a reboot
: Type the following command on one line

start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery.msi" /qn
```

インストール後に再起動しない場合は、次のコマンドを実行します。

```
: Silent install using the MSI without a reboot
: Type the following command on one line

start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery.msi" /qn REBOOT="R"
```

3. 次のコマンドを実行します。

```
: Start the Rescue and Recovery Service
net start  "TVT Backup Service"

: Create Sysprep Base Backup to Local Hard Drive
: Type the following command on one line

cd "¥Program Files¥Lenovo¥Rescue and Recovery"
rrcmd sysprepbackup location=l name=Sysprep Backup"
```

パスワードを使用する場合は、構文 password=*pass* を追加します。

4. 次のメッセージが表示されたら、Sysprep を実行します。

```
***************************************************
** Ready to take sysprep backup.               **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.        **
**                                              **
** Next time the machine boots, it will boot     **
** to the Predesktop Area and take a backup.     **
***************************************************
```

5. Sysprep が完了すると、PC がシャットダウンされますので、PC の電源を再度オンにします。

   注: オペレーティング・システムが再起動して、Rescue and Recovery ワークスペースに入ります。「**システムの復元中**」というステータス・バーが表示されます。
6. 完了すると、「**The Sysprep Backup is Complete**」というメッセージが表示されます。
7. 「再起動」ボタンを押して再起動します。
8. デプロイメント用のイメージを取り込みます。

複数パーティションを持つ PC の取り込みと、Sysprep イメージ内のファイルを除外

Sysprep イメージで複数のパーティションを取り込むには、次のようにします。

1. 次のようにして管理用インストール・アクションを実行します。

```
:: Extract the WWW EXE to the directory C:¥TVTRR
start /WAIT setup_tvtrnr_xxxx.exe /a /s /v"/qn TARGETDIR
(where XXXX is the build ID)
="C:¥TVTRR" REBOOT="R"" /w
```

2. C:¥tvtrr¥Program Files¥Lenovo¥Rescue and Recovery にある rnrdeploy.xml ファイルの末尾に次のコマンドを追加します。

```
<Rescue__and__Recovery..Settings..Backup path
="Rescue and Recovery¥Settings¥Backup">
```

パーティションを除外するには、rnrdeploy.xmlファイルに以下のセクションを追加します。

```
<BackupPartitions dword="20" />
</Rescue__and__Recovery..Settings..Backup>
```

rnrdeploy.xml ファイルの使用法について詳しくは、「ThinkVantage Technologies XML/ADM Supplement」を参照してください。この資料は、Lenovo Web サイト http://www.lenovo.com/thinkvantage (英語のサイトです) からダウンロードできます。「Support and Downloads」→「User's Guides and Manuals」の順にクリックし、「Brand」で「ThinkVantage Technologies」を、「Family」で「Rescue and Recovery」を選択してから「Continue」をクリックします。

3. バックアップから .mpg および .jpg ファイルを除外するには、HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥BackupList にあるレジストリー項目でそれらを含めるように設定します。レジストリーを使用するバックアップの包含と除外について詳しくは、 16 ページの『レジストリー設定を使用するバックアップ・ファイルの包含と除外』を参照してください。
4. MSIEXE を使用して Rescue and Recovery をインストールするには:
   a. すべての MSI ファイルで次のインストール・ログ生成コードを追加します。

      ```
      /L*v %temp%¥rrinstall.txt
      ```

   b. MSIEXE を使用してインストールするには、次のコマンドを実行します。

      ```
      : Perform the install of Rescue and Recovery

       msiexec /i "C:¥TVTRR¥Rescue and Recovery.msi"
      ```

   c. MSIEXE を使用してサイレント・インストールするには:

      最後に起動をする場合は、次のコマンドを実行します。

      ```
      : Silent install using the MSI with a reboot

      : Type the following command on one line
      start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery.msi" /qn
      ```

      インストール後に再起動しない場合は、次のコマンドを実行します。

      ```
      : Silent install using the MSI without a reboot

      : Type the following command on one line
      start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery.msi" /qn REBOOT="R"
      ```

5. 次のコマンドを実行します。

   ```
   :Start the Rescue and Recovery Service
   net start  "TVT Backup Service"

   :Create Sysprep Base Backup to Local Hard Drive

   : Type the following command on one line

   cd "¥Program Files¥Lenovo¥Rescue and Recovery"
   rrcmd sysprepbackup location=L name="Sysprep Base Backup"
   ```

パスワードを使用する場合は、構文 password=*pass* を追加します。

6. 次のメッセージが表示されたら、Sysprep を実行します。

```
***************************************************
** Ready to take sysprep backup.                **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.        **
**                                              **
** Next time the machine boots, it will boot    **
** to the Predesktop Area and take a backup.    **
***************************************************
```

7. Sysprep が完了すると、PC がシャットダウンされますので、PC の電源を再度オンにします。

   注: オペレーティング・システムが再起動して、Rescue and Recovery ワークスペースに入ります。「**システムの復元中**」というステータス・バーが表示されます。

8. 完了すると、「**The Sysprep Backup is Complete**」というメッセージが表示されます。
9. 「再起動」ボタンを押して再起動します。
10. デプロイメント用のイメージを取り込みます。

Windows 環境での Rescue and Recovery の使用

Windows 環境で Rescue and Recovery プログラムを使用すると、多くのタイプのバックアップを実行できます。次の情報は、Rescue and Recovery でバックアップ・ファイルを使用する方法について説明しています。

レジストリー設定を使用するバックアップ・ファイルの包含と除外

Rescue and Recovery は、個別のファイル、個別のフォルダー、または区画全体を包含および除外することができます。Rescue and Recovery バージョン 3.1 では、これらの機能はタイプ REG_MULTI_SZ の次のレジストリー項目によって制御されます。

- HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥BackupList
- HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥ExcludeList
- HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥OSAppsList

基本バックアップの場所の設定

インストールが完了するとすぐに、次のレジストリー項目によって基本バックアップが設定されます。

```
HKLM¥Software¥Lenovo¥Rescue and Recovery¥runbasebackuplocation
DWord = location value
```

BackupList

レジストリー項目のフォーマットは、次のとおりです。

HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥BackupList

- 包含/除外につき 1 行の規則の入力。
- ファイルまたはフォルダーに複数の設定が適用される場合は、最後に適用された設定が使用されます。レジストリー項目の下部の入力が優先されます。

- 入力は、次のいずれかで記述する必要があります。
  - **;**

    は、コメント行です。
  - **I**

    は、その入力に一致するファイルまたはフォルダーを包含します。
  - **X**

    は、その入力に一致するファイルまたはフォルダーを除外します。
  - **S**

    は、ファイルまたはフォルダー上に Single Instance Storage を包含します。
  - **i**

    は、包含するように選択することができるファイルまたはフォルダー用です。
  - **x**

    は、除外するように選択することができるファイルまたはフォルダー用です。
  - **s**

    は、ユーザーが Single Storage に追加することを選択できるファイルまたはフォルダーです。

以下は、入力の例です。

```
  S=*
  X=*
  i=*
I=*.ocx
I=*.dll
I=*.exe
I=*.ini
I=*.drv
I=*.com
I=*.sys
I=*.cpl
I=*.icm
I=*.lnk
I=*.hlp
I=*.cat
I=*.xml
I=*.jre
I=*.cab
I=*.sdb
I=*.bat
I=?:¥ntldr
I=?:¥peldr
I=?:¥bootlog.prv
I=?:¥bootlog.txt
I=?:¥bootsect.dos
I=?:¥WINNT¥*
I=?:¥WINDOWS¥*
X=?:¥WINDOWS¥prefetch¥*
I=?:¥minint¥*
I=?:¥preboot¥*
I=?:¥Application Data¥*
I=?:¥Documents and Settings¥*
I=?:¥Program Files¥*
```

```
I=?:¥msapps¥*
  X=?:¥Recycled
  X=?:¥RECYCLER
  x=?:¥Documents and Settings¥*¥Cookies¥*
x=?:¥Documents and Settings¥*¥Local Settings¥History¥*
X=?:¥Documents and Settings¥*¥Local Settings¥Temp¥*
x=?:¥Documents and Settings¥*¥Local Settings¥Temporary Internet Files¥*
x=?:¥Documents and Settings¥*¥Desktop¥*
x=?:¥Documents and Settings¥*¥My Documents¥*
  s=?:¥Documents and Settings¥*¥Desktop¥*
  s=?:¥Documents and Settings¥*¥My Documents¥*
  x=*.vol
  s=*.vol
```

ExcludeList

レジストリーのこのセクションでは、Rescue and Recovery によって開始されたリカバリー・プロセスからソフトウェア・アプリケーションを除外することを選択できます。この GUI の除外リストは、HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥ExcludeList にあるレジストリーによって管理されます。

OSAppsList

Rescue and Recovery バージョン 3.1 は、次のレジストリー・キー設定を使用して OS とアプリケーションを復元する場合に特定のファイルおよびフォルダーを選択して復元する機能を提供します。

HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥OSAppsList

OSAppsList 設定は、どのファイル、フォルダー、またはファイル・タイプがオペレーティング・システムおよびアプリケーションを構成するか定義します。このファイルは管理者によってカスタマイズすることができ、デフォルトの外部ファイルが提供されます。ユーザーがオペレーティング・システムのリカバリーを選択すると、この外部ファイルに含まれている規則に一致するファイルのみ復元するオプションを選択可能なメニューが表示されます。管理者は、この外部ファイルの内容をカスタマイズできます。

Rescue and Recovery のその他の側面のカスタマイズ

Rescue and Recovery バージョン 3.1 では、設定のカスタマイズはレジストリーおよび rnrdeploy.xml ファイルを使用して行われます。レジストリー設定が含まれる XML ファイルを表示するには、rnrdeploy.xml ファイルを http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMDL (英語のサイトです。) からダウンロードします。

Active Directory を使用する企業のお客様は、153 ページの『Active Directory のサポート』を参照してください。

障害報告

ファイル転送または電子メールを介して Rescue and Recovery 環境から情報を送信する方法はありません。エンド・ユーザーは、ブラウザーに統合された電子メール機能の使用を指示されます。ロギング機能はログ・イベントをファイルにパッケージして、エンド・ユーザーがリカバリー・プロセスを完了して Windows にログオンした後にファイルを電子メールで送信するように指示します。エンド・ユーザーから受信するファイルによって、*Req 115 障害報告票* の XML ファイルが作成され

ます。このファイルは「システム情報」に表示されるすべての情報 (現在のハードウェア、eGatherer、および PCDR 診断ログ情報) を組み合わせたもので、Rescue and Recovery 環境およびオペレーティング・システム - C:¥SWSHARE の両方から容易にアクセス可能な場所に置かれます。

Rescue and Recovery ワークスペースで使用可能な診断ツールは、問題判別を支援します。診断ツールによって実行されるテストからの出力は、ヘルプ・デスクに表示または伝送できる方法で保存されます。

ワークスペース (Predesktop Area)

Rescue and Recovery ワークスペース (Predesktop Area) の一部をカスタマイズするには、rrutil.exe ユーティリティー・プログラムを使用して、Rescue and Recovery ワークスペースまたは保護されたバックアップ・フォルダーからファイルを抽出・適用します。

注: オペレーティング・システムが起動しない場合でも、Rescue and Recovery ワークスペースを手動で開始できます。
これらのファイルまたはディレクトリーおよびそれらのカスタマイズ・オプションは、次の表にリストされています。

表 1. RRUTIL.exe ファイルおよびカスタマイズ・オプション

ファイルまたはディレクトリー	カスタマイズ・オプション
¥MININT¥SYSTEM32 WINBOM.INI	固定 IP アドレスの追加、画面の解像度の変更 **注:** Rescue and Recovery の winbom.ini ファイルをカスタマイズする場合、すべての winbom.ini ファイルをカスタマイズする必要があります。
¥MININT¥INF ¥MININT¥SYSTEM32¥DRIVERS	デバイス・ドライバーの追加
MAINBK.BMP	Rescue and Recovery ワークスペース画面の背景の変更
MINIMAL_TOOLBAR(1).INI	アドレス・バーの無効化
NORM1.INI	Opera ブラウザーの設定、Opera アドレス・バーの無効化、Opera プロキシー設定の変更、修正ダウンロード・フォルダーの指定、ダウンロード可能なファイル・リストへの特定のファイル拡張子の追加、特定の拡張子を持つファイルの動作の変更
OPERA_010.CMD	Windows ユーザーのお気に入りの除外
OPERA6.INI	Opera ブラウザーの設定、アドレス・バーの無効化
PDAGUI*xx*.INI (ここで、*xx* は言語の指定です)	Rescue and Recovery ワークスペース内の GUI フォント、環境背景、左右パネルの項目と機能、HTML ベースのヘルプ・システムの設定
STANDARD_MENU.INI	「名前を付けて保存」ウィンドウの表示の有効化

RRUTIL.EXE の使用

RRUTIL プログラムは、Rescue and Recovery のサービス区画および仮想パーティション・データにアクセスするよう設計されています。このユーティリティーは、仮

想パーティションおよびタイプ 12 区画の両方で機能します。管理者は、このユーティリティーを使用して Rescue and Recovery ワークスペース (PDA) をカスタマイズすることができます。デフォルトで、このツールを使用できるのは管理者ユーザーのみです。

rrutil.exe は次の Web サイトから入手できます。

http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN

RRUTIL プログラムは、仮想パーティション上の Rescue and Recovery フィルター・ドライバーと連動して、アクセスを取得するためにタイプ 12 区画をドライブとしてマウントします。これらの区画を開くには、要求されたコマンドを実行してから再び閉じるのに十分な時間しかかかりません。

このプログラムでは、管理者は以下の機能を実行できます。

- Rescue and Recovery ワークスペースのディレクトリーを表示する。
- Rescue and Recovery ワークスペースでファイルを追加または更新する。
- Rescue and Recovery ワークスペースからファイルを削除する。
- Rescue and Recovery ワークスペースのファイルを名前変更する。
- ¥RRbackups ディレクトリーのファイルを表示する。
- ¥RRbackups ディレクトリーからバックアップを削除する。
- ¥RRbackups ディレクトリーにバックアップを追加する。
- ¥RRbackups ディレクトリーからファイルを取得する。
- ¥RRbackups ディレクトリーのディスク・スペース使用量を表示する。

Rescue and Recovery ワークスペースのディレクトリー・リスト

```
RRUTIL /lx [<path>dirlist.txt]
```

次のようにして、Rescue and Recovery ワークスペースの仮想またはタイプ 12 の ¥preboot、¥minint、またはルート・ディレクトリーの内容のリストを作成します。

1. データは、ユーザーが指定するディレクトリー名にある dirlist.txt というファイルに各サブディレクトリーの全ファイルのテキスト・ストリームとして書き込まれるか、パスが指定されない場合は c:¥ のルートに書き込まれます。
2. これは、該当するディレクトリーで次の DOS 形式のコマンド (“dir * /s > c:¥temp¥dirlist.txt”) を実行することに相当します。PE 区画のルートの内容をリストする場合は、“dir * > c:¥temp¥dirlist.txt” のみです。出力例:

```
Directory of ¥

10/20/03 00:00:00 AM         42    AUTOEXEC.ICR
03/12/04 00:00:00 AM         42    AUTOEXEC.bat
03/10/04 00:00:00 AM        165    BOOT.INI
08/16/02 00:00:00 AM      53786    COMMAND.COM
12/16/03 00:00:00 AM        222    CONFIG.ICR
12/16/03 00:00:00 AM        222    CONFIG.SYS
04/06/00 00:00:00 AM        655    FINDDRV.BAT
09/17/03 00:00:00 AM      14320    HIMEM.SYS
```

3. オプションのコマンド・ライン入力は、このオプションの出力を取り込むテキスト・ファイルです。
4. サンプル・コマンド: RRUTIL /lx [<path>dirlist.txt] *注: オプション入力の有効化は後のリリースまで据え置かれる可能性があります。

```
x  result listing
1  ¥preboot
2  ¥minint
4  <root of c:¥ or root of type 12 partition>
```

複数のリストを作成するには、単にそれぞれの x を加算します。そのため、¥preboot および ¥minint は値 3 になります。dirlist.txt の内容は次のとおりです。

```
¥minint¥system32¥drivers*.sys
¥preboot¥startup¥*.*
```

Rescue and Recovery ワークスペース・ディレクトリーからのファイルの取得

```
RRUTIL /g <path>getlist.txt <copy to location>
```

次のようにして、仮想またはタイプ 12 の PE 区画の ¥preboot、¥minint、またはルートから個別ファイルをコピーします。

1. テキスト・ファイルは、コマンド・ラインで指定された場所にコピーされるファイルを識別します。
2. <copy to location> は、Rescue and Recovery ワークスペースからファイルを受け取る既存ディレクトリーでなければなりません。ファイルは、このディレクトリーに Rescue and Recovery ワークスペースで検出されるのと同じツリー構造でコピーされます。これによって、同じ名前のファイルを相互に上書きコピーすることが回避されます。
3. サンプル・コマンド: RRUTIL /g <path> getlist.txt <copy to location> getlist.txt の内容は次のとおりです。

```
¥PELDR
 ¥preboot¥startup¥Restore.cmd
 ¥preboot¥usrintfc¥PDAGUI.ini
```

注: この関数ではワイルドカードはサポートされません。変更を試行する前に、Rescue and Recovery ワークスペースについて理解する必要があります。

Rescue and Recovery ワークスペース・ディレクトリーへのファイルの書き込み

```
RRUTIL /p <path>
```

次のようにして、仮想またはタイプ 12 の PE 区画の ¥preboot、¥minint、またはルートにあるファイルを更新 (追加/置換) します。

1. ドライブ c:¥ の一時フォルダーにすべてのファイルを置きます。一時ディレクトリーの場所に従って、ファイルは PE 区画の同じ場所にコピーされます。たとえば、¥preboot¥startup の file.cmd ファイルを追加/置換するには、file.cmd ファイルを c:¥tempdir¥preboot¥startup に置いてから、コマンド "RRUTIL /p c:¥tempdir" を実行します。
2. サンプル・コマンド: RRUTIL /p c:¥PDATemp c:¥PDATemp の内容は、Rescue and Recovery ワークスペースの ¥preboot、¥minint、またはルートのディレクトリー構造のミラー・イメージです。c:¥PDATemp のルートにあるファイルは、PE 区画のルートにファイルを書き込みます。

Rescue and Recovery ワークスペース・ディレクトリーからのファイルの削除

```
RRUTIL /d C:¥temp¥dellist.txt
```

次のようにして、仮想またはタイプ 12 の Rescue and Recovery 区画の ¥preboot、¥minint、またはルートにあるファイルを削除します。

1. テキスト・ファイルの内容に基づいて、仮想またはタイプ 12 の PE 区画の ¥preboot、¥minint、またはルートにあるファイルを削除します。
2. Dellist.txt に、PDA から削除されるファイルのツリー構造が含まれている必要があります。
3. サンプル・コマンド: RRUTIL /d <path> dellist.txt dellist.txt の内容は次のとおりです。

```
¥preboot¥startup¥custom.cmd  Sample file name only
¥preboot¥usrintfc¥test.txt  Sample file name only
```

Rescue and Recovery ワークスペースのファイル名の変更

```
RRUTIL /r ¥<PDA-path>¥oldfilename.ext newfilename.ext
```

Rescue and Recovery ワークスペースにあるファイルを名前変更します。この機能は、Rescue and Recovery ワークスペースにあるファイルでのみ実行できます。名前変更するファイルへのパスをドライブ名なしで含める必要があります。ファイルの新しい名前には、パス情報が入っていない名前のみを含める必要があります。

例:

```
RRUTIL -r ¥preboot¥usrintfc¥peaccessibmen.ini peaccessibmen.old
```

インストール済みの Rescue and Recovery のテスト

```
RRUTIL /bq
```

このコマンドは、自動処理を支援するためにバッチ・ファイルで使用できます。Rescue and Recovery コードがシステムのみにインストールされていない場合、Rescue and Recovery ワークスペースにアクセスする機能を使用できます。

例:

```
RRUTIL -bq
```

環境変数 %errorlevel% の結果は、Rescue and Recovery がシステムにインストールされていない場合は -2、または Rescue and Recovery がインストールされている場合は 0 に設定されます。echo %errorlevel% と入力して、コマンドの結果を確認します。

バックアップ・ディレクトリーのリスト

```
RRUTIL /bl <path>
```

¥RRbackups ディレクトリーのすべての内容をリストします。バックアップの各ファイルのファイル・サイズ、日付、および場所を表示します。下記のリストは、基本バックアップと増分バックアップ 1 つのバックアップ・ディレクトリーの例です。

```
Directory of ¥RRbackups¥C¥0¥

03/11/04 08:02:44 AM   50003968    Data0
03/11/04 08:04:05 AM   50003968    Data1
03/11/04 08:07:10 AM   50003968    Data10
03/11/04 09:09:03 AM   50003968    Data100
03/11/04 09:10:39 AM   50003968    Data101
03/11/04 09:12:07 AM   50003968    Data102
03/11/04 09:13:24 AM   50003968    Data103
03/11/04 08:01:31 AM               EFSFile
03/15/04 22:22:47 PM     338772    HashFile
03/11/04 09:17:44 AM        748    Info
03/15/04 22:22:47 PM   34443040    TOCFile

Directory of ¥RRbackups¥C¥1¥

03/15/04 22:29:29 PM   50003968    Data0
03/15/04 22:29:45 PM   50003968    Data1
03/15/04 22:44:50 PM   50003968    Data10
03/15/04 22:51:56 PM   50003968    Data11
03/15/04 22:56:39 PM   50003968    Data12
03/15/04 23:00:27 PM   43480478    Data13
03/15/04 22:30:00 PM   50003968    Data2
03/15/04 22:30:19 PM   50003968    Data3
03/15/04 22:30:34 PM   50003968    Data4
03/15/04 22:30:57 PM   50003968    Data5
03/15/04 22:32:25 PM   50003968    Data6
03/15/04 22:33:42 PM   50003968    Data7
03/15/04 22:34:40 PM   50003968    Data8
03/15/04 22:42:57 PM   50003968    Data9
03/15/04 22:22:47 PM               EFSFile
03/15/04 23:00:27 PM     374742    HashFile
03/15/04 23:00:27 PM        748    Info
03/15/04 23:00:27 PM   38099990    TOCFile
```

¥RRBackups ディレクトリーからのファイルの取得

```
RRUTIL /bg <path>getlist.txt <copy to location>
```

¥RRbackups ディレクトリーから個別ファイルをコピーします。

1. テキスト・ファイルは、コマンド・ラインで指定された場所にコピーされるファイルを識別します。
2. <copy to location> は、¥RRbackups ディレクトリーからファイルを受け取る既存ディレクトリーでなければなりません。ファイルは、このディレクトリーに ¥RRbackups ディレクトリーで検出されるのと同じツリー構造でコピーされます。
3. サンプル・コマンド: RRUTIL /bg <path> getlist.txt <copy to location> getlist.txt の内容は次のとおりです。

   注: この関数ではワイルドカードはサポートされません。変更を試行する前に、¥RRbackups ディレクトリー環境について理解する必要があります。

¥RRBackups ディレクトリーへのファイルの書き込み

```
RRUTIL /bp <path>
```

¥RRbackups 仮想パーティションにあるファイルを更新 (追加/置換) します。

1. ドライブ c:¥ の一時フォルダーにすべてのファイルを置くと、一時ディレクトリーの場所に従って、ファイルは ¥RRbackups ディレクトリーの同じ場所にコピーされます。
2. サンプル・コマンド: RRUTIL /bp c:¥RRTemp。c:¥RRTemp の内容は、ファイルが移動する ¥RRbackups ディレクトリー構造のミラー・イメージです。

   ```
   C:¥RRTemp¥C¥0 Data0 Data1
    EFSFile HashFile Info TOCFile
   ```

   から

   ```
   C:¥RRbackups¥C¥0 Data0  Data1
    EFSFile HashFile Info TOCFile
   ```

¥RRBackups ディレクトリーからのバックアップ・ファイルの削除

```
RRUTIL /br ¥RRbackups¥C¥0
```

この機能は、指定されたディレクトリーのファイルの削除のみを行います。Rescue and Recovery アプリケーションのバックアップ削除機能の代わりに使用してはなりません。この機能を見境なく使用すると、注意深く使用されない場合には、システムで Rescue and Recovery アプリケーションによって認識されているすべてのバックアップが破棄される可能性があります。

この機能は、不良であると疑われるバックアップ・ファイル・セットを削除して、代替メディアに保管されている元のファイルと置き換える場合に使用できます。基本バックアップを管理者が維持する基本バックアップと交換するために、この機能を使用できます。基本バックアップが全システムで同じであり、更新とパッチを必要とする場合があります。

1. 指定されたバックアップ・ディレクトリーの内容を削除します。
2. サンプル・コマンド: RRUTIL /br ¥RRbackups¥C¥0 を実行すると、このディレクトリーのすべてのバックアップ・ファイルが削除されます。

¥RRBackups スペース消費量の判別

```
RRUTIL /bs
```

¥RRbackups により消費されているスペースの量を判別します。

1. バックアップにより消費されているスペースの量を判別できます。バックアップごとに (たとえば、基本およびそれぞれの増分) スペースの消費量がリストされます。
2. サンプル・コマンド: RRUTIL /bs を実行すると、コンソールにバックアップ・スペースが表示されます。

本章で前述したように、rrutil.exe ファイルを使用すると、Rescue and Recovery 環境からファイルを取得したり、ファイルを書き込むことができ、Rescue and Recovery 環境およびバックアップ・フォルダーにあるファイルをリストすることもできます。これらの手順は、Rescue and Recovery ワークスペースのすべてのファイ

ル・カスタマイズで同じです。次の手順では、Rescue and Recovery 環境で取得および書き込みの機能を使用する方法について別の例を示します。

rrutil.exe を使用するには、次の操作を行います。

1. rrutil.exe を C ドライブのルートにコピーします。
2. getlist.txt ファイルを次の構文で作成します。

   ```
   ¥preboot¥usrintfc¥file name
   ```

   ファイルを c:¥temp¥getlist.txt として保存します。
3. コマンド・プロンプトで、rrutil.exe コマンド、および下表で定義されているいずれか 1 つのスイッチを入力します。その後、次の表に示されるような適切なパラメーターを指定してコマンドを入力します。

表 2. コマンドおよびスイッチ・オプション

コマンドおよびスイッチ・オプション	結果
RRUTIL -l1	preboot フォルダーの内容を表示する。
RRUTIL -l2	minint フォルダーの内容を表示する。
RRUTIL -l4	C ドライブのルートまたはタイプ 12 区画のルート (工場出荷時に Rescue and Recovery がプリロードされているモデル) の内容を表示する。
RRUTIL -g c:¥temp¥getlist.txt C:¥temp	Rescue and Recovery ワークスペースからファイルを取得する。
RRUTIL -d c:¥temp¥ dellist.txt	Rescue and Recovery ワークスペースからファイルを削除する
RRUTIL -p c:¥temp	Rescue and Recovery ワークスペースにファイルを追加または置換する
RRUTIL -r *path* ¥*oldname.ext newname.ext* RRUTIL -r ¥temp¥rr¥test.txt test2.txt ファイルは preboot¥rr フォルダー内にあります。	ワークスペースのファイルを名前変更する。
RRUTIL -bp c:¥temp	RRBACKUPS 仮想パーティションのファイルを更新または置換する。
RRUTIL -bl *path* RRUTIL -bl は c:¥rr-list.txt にリストする。 rrutil -bl c:¥rrtemp	RRBACKUPS ディレクトリーをリストする。
RRUTIL -br RRbackups¥C¥n ここで n はバックアップ数。	バックアップの内容を削除する
RRUTIL -bg c:¥temp¥bgetlist.txt C:¥temp	¥RRBACKUPS から個別ファイルをコピーする。
RRUTIL -bs	RRBackups ディレクトリーにより使用されているスペースを表示する。

4. ファイルを取得した後は、標準的なテキスト・エディターを使用してファイルを編集できます。

例: pdaguixx.ini

この例は pdagui*xx*.ini を参照しています。これは、Rescue and Recovery 環境のエレメントをカスタマイズできる設定ファイルです (27 ページの『Rescue and Recovery ワークスペースのカスタマイズ』を参照してください)。

注: ファイル名にある *xx* は、以下の 2 文字の言語省略語を表しています。

表 3. 言語コード

2 文字の言語コード	言語
br	ブラジル・ポルトガル語
dk	デンマーク語
en	英語
fi	フィンランド語
fr	フランス語
gr	ドイツ語
it	イタリア語
jp	日本語
kr	韓国語
nl	オランダ語
no	ノルウェー語
po	ポルトガル語
sc	中国語 (簡体字)
sp	スペイン語
sv	スウェーデン語
tc	中国語 (繁体字)

Rescue and Recovery ワークスペースからのファイル pdaguien.ini の取得

1. 次の行を含んだ getlist.txt ファイルを作成します。
```
\preboot\reboot\usrintfc\pdaguien.ini
```
2. ファイルを c:¥temp¥getlist.txt として保存します。
3. コマンド・プロンプトで、次のコマンドを実行します。
```
c:\RRUTIL-g c:\temp\getlist.txt c:\temp
```

ファイル pdaguien.ini を元の Rescue and Recovery ワークスペースに適用します

コマンド・プロンプトで、次のコマンドを実行します。

```
C:\RRUTIL.EXE -p c:\temp
```

注: 適用コマンド (**-p**) は、取得コマンド (**-g**) で作成されたフォルダー構造を使用します。編集したファイルを適切に配置するために、次の例のように、編集されたファイルが getlist.txt ファイルと同じフォルダーに置かれていることを確認してください。

```
c:\temp\preboot\usrintfc\pdaguien.ini
```

例 1: ワークスペースへのデバイス・ドライバー (イーサネットなど) の追加

次の例は、ワークスペースにデバイス・ドライバーを追加する手順を示しています。

1. デバイス・ドライバーをベンダーの Web サイトまたはその他のメディアから入手します。
2. 以下のフォルダーを作成します。

   ```
   C:¥TEMP¥MININT¥INF
   C:¥TEMP¥MININT¥SYSTEM32¥DRIVERS
   ```
3. ネットワーク・ドライバーの *.inf ファイルを ¥MININT¥INF フォルダーにコピーします。(たとえば、E100B325.inf は ¥MININT¥INF フォルダーに置く必要があります。)
4. すべての *.sys ファイルを ¥MININT¥SYSTEM32¥DRIVERS ディレクトリーにコピーします。(たとえば、E100B325.sys は ¥MININT¥SYSTEM32¥DRIVERS フォルダーに置く必要があります。)
5. 関連する *.dll、*.exe、またはその他のファイルを ¥MININT¥SYSTEM32¥DRIVERS フォルダーにコピーします。(たとえば、E100B325.din または INTELNIC.dll ファイルは、¥MININT¥SYSTEM32¥DRIVERS フォルダーに置く必要があります。)

   注:
   a. カタログ・ファイルは Rescue and Recovery ワークスペースで処理されないため、不要です。上記の手順は、PC を設定するために必要なすべてのデバイス・ドライバーにあてはまります。
   b. Rescue and Recovery ワークスペースの制限により、一部のアプリケーションまたは設定はレジストリー更新として手動で行う必要があります。
6. デバイス・ドライバーを Rescue and Recovery ワークスペースに配置するには、コマンド・プロンプトから以下を実行します。

   ```
   C:¥ RRUTIL.EXE -p C:¥temp
   ```

例 2: ワークスペースへの大容量ストレージ・コントローラー・ドライバー (SATA など) の追加

1. ¥minint¥system32¥ の下にドライバーを入れるサブディレクトリーを作成します。
2. *.sys を ¥minint¥systme32¥drivers にコピーします。
3. ¥minint¥system32¥winpeoem.sif を更新して、ドライバーが入ったサブディレクトリーが含まれるようにします (たとえば、このファイルを 3.0 ビルド 37 から検査します)。
4. iastor ファイルおよびフォルダーが、作成されたサブディレクトリーにあることを確認します。
5. iastor ドライバーが含まれる作成済みサブディレクトリーに有効な txtsetup.oem ファイルが入っていることを確認してください。

Rescue and Recovery ワークスペースのカスタマイズ

設定ファイル pdagui*xx*.ini (ここで、*xx* は言語の指定です) を編集して、Rescue and Recovery 環境の以下のエレメントをカスタマイズできます。

- GUI フォントの変更
- Rescue and Recovery ワークスペース画面の背景の変更
- Rescue and Recovery ワークスペースの左パネルにある項目および機能
- Rescue and Recovery ワークスペース内の HTML ベースのヘルプ

注: pdaguien.ini ファイルの取得、編集、および置換については、26 ページの『例: pdaguixx.ini』を参照してください。

GUI フォントの変更

Rescue and Recovery ワークスペース上の GUI のフォントを変更することができます。デフォルト設定では、必要な言語および文字によって、すべてが正確に表示されない場合があります。初期設定は pdagui*xx*.ini (ここで、*xx* は言語の指定です) の [Fonts] セクションに記述されています。以下は、日本語用の初期設定値です。

```
[Fonts]

LeftNavNorm = "MS UI Gothic"

LeftNavBold = "Arial Bold"

MenuBar = "MS UI Gothic"
```

以下のフォントは Rescue and Recovery ワークスペースと互換性があり、テスト済みです。

- Courier
- Times New Roman
- Comic Sans MS

その他のフォントの互換性に関して Lenovo では動作確認をしておりません。

Rescue and Recovery ワークスペースの背景の変更

右パネルの背景はビットマップ・グラフィックで、mainbk.bmp という名前が付けられています。ファイル mainbk.bmp は ¥PREBOOT¥USRINTFC フォルダーに置かれています。右パネルの背景用に独自のビットマップ・イメージを配置する場合、以下のサイズに準拠している必要があります。

- 幅 620 ピクセル
- 高さ 506 ピクセル

Rescue and Recovery で希望の背景を表示するには、ファイルを ¥PREBOOT¥USRINTFC フォルダーに置く必要があります。

注: mainbk.bmp ファイルの取得、編集、および置換については、19 ページの『RRUTIL.EXE の使用』を参照してください。

pdagui.ini の編集

左パネルの項目を変更するには、pdagui*xx*.ini (ここで、*xx* は言語の指定です) ファイルを編集する必要があります。Rescue and Recovery 環境から pdagui*xx*.ini を取得して、ファイルを置換する方法については、19 ページの『RRUTIL.EXE の使用』を参照してください。

Rescue and Recovery の左パネルには 21 の項目があります。各項目の機能は異なりますが、基本となる構文は同じです。以下に、左パネルの項目の例を示します。

```
[LeftMenu] button00=2, "Introduction", Introduction.bmp, 1,

1, 0, %sysdrive%¥Preboot¥Opera¥ENum3.exe,
```

表 4. 左パネルの項目およびカスタマイズ・オプション

項目	カスタマイズ・オプション
00-01	完全にカスタマイズ可能。

表 4. 左パネルの項目およびカスタマイズ・オプション (続き)

項目	カスタマイズ・オプション
02	ボタン・タイプは 1 のままである必要がある (表 5 を参照)。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
03-06	完全にカスタマイズ可能。
07	ボタン・タイプは 1 のままである必要がある。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
08-10	完全にカスタマイズ可能。
11	ボタン・タイプは 1 のままである必要がある。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
16	ボタン・タイプは 1 のままである必要がある。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
17-22	完全にカスタマイズ可能。

ボタン・タイプの定義: `Button00` の数字は他と重なってはいけません。若い数字の順で、左パネルに表示されます。

`Button00=[0-8]` このパラメーターでボタン・タイプを決定します。この値は、0 ～ 8 まで指定できます。次の表に、各ボタン・タイプの値と動作が記載されています。

表 5. 項目タイプ・パラメーター

パラメーター	説明
`0`	空フィールド。この値は、行を空白または未使用のまま残す場合に使用します。
`1`	セクションの見出しテキスト。この設定は、主なグループまたはセクションの見出しを設定する場合に使用します。
`2`	アプリケーションの起動。ユーザーがボタンまたはテキストをクリックすると起動されるアプリケーションまたはコマンド・ファイルを定義します。
`3`	Rescue and Recovery ワークスペースの Opera ヘルプ。 Opera ブラウザーのヘルプ・トピックを定義します。
`4`	起動前に再起動メッセージ・ウィンドウを表示する。値を変更すると、GUI は指定された機能を実行する前に PC を再起動する必要があるというメッセージをユーザーに表示します。
`5`	未使用
`6`	未使用
`7`	起動して待機します。この値を使用すると、Rescue and Recovery ワークスペースが続行する前に起動されたアプリケーションの戻り値を待つことを強制します。戻り値は、環境変数 %errorlevel% に返されます。

表 5. 項目タイプ・パラメーター (続き)

パラメーター	説明
8	アプリケーションの起動。GUI はアプリケーションを起動する前に、国別コードと言語を検索します。CGI スクリプトを含む Web リンクが特定の国または特定の言語の Web ページを開くために使用されます。
9	未使用
10	未使用

入力フィールドの定義:

`Button00=[0-10], "title"`
: ボタン・タイプ・パラメーターに続くテキストにより、ボタンのテキストまたはタイトルが指定されます。テキストが左パネルの幅よりも大きい場合、テキストは切り取られ、省略符号ポイントによりさらに文字が続くことが示されます。吹き出しヘルプを使用しているときは、完全なタイトル・テキストが表示されます。

`Button00=[0-10], "title", file.bmp`
: タイトル・テキストの前に表示される前に表示されるアイコンとして使用するビットマップのファイル名を指定します。ビットマップのサイズは、15 ピクセル x 15 ピクセル以下でなければなりません。

`Button00=[0-10], "title", file.bmp, [0 or 1]`
: Rescue and Recovery ワークスペースで項目を表示するか、非表示にするかを設定します。値 `0` を設定すると、項目は非表示になり、空白行が表示されます。値 `1` を設定すると、項目は表示されます。

`Button00=[0-10], "title", file.bmp, [0 or 1], 1`
: これは予備の機能であり、常に `1` に設定する必要があります。

`Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1]`
: 項目を起動する前にパスワードを要求するには、`1` を指定します。この値を `0` に設定すると、項目を起動する前にパスワードは要求されません。

`Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1], %sysdrive%[pathname¥executable]`
: `%sysdrive%` の値は、起動ドライブ名でなければなりません。起動ドライブ名の後に、アプリケーションまたはコマンド・ファイルの完全修飾パスを指定します。

`Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1],%sysdrive%[pathname¥executable], [parameters]`
: 起動しているアプリケーションまたはコマンドに必要とされるパラメーターを指定します。

これらのフィールドに値を指定しない場合、ボタンが正常に実行されるように、必要な数のコンマを入力する必要があります。たとえば、″Rescue and Recover″ というグループ見出しを作成する場合、以下のように指定します。

```
Button04=1, "Rescue and Recover",,,,,,
```

項目 02、07、11 および 16 はタイプ 0 (または見出し) 項目のままにする必要があり、常にその数値的空間に整列しています。見出しの下に続く有効な項目の数を減らすには、完全にカスタマイズ可能な項目をタイプ 0、つまり左パネルの空白行に設定します。ただし、項目の総数は 23 を超えてはなりません。

次の表はデフォルトで、左パネルの項目から起動できる機能および実行可能ファイルを示しています。

表 6. 左パネルの機能および実行可能ファイル

機能	実行可能ファイル
ファイルのレスキュー	WIZRR.EXE
システムの復元	WIZRR.EXE
移行ファイルの作成	WIZRR.EXE
ブラウザーを開く	OPERA.EXE
ネットワーク・ドライブの割り当て	MAPDRV.EXE
ハードウェアの診断	RDIAGS.CMD; PC Doctor アプリケーションを起動します。IBM® および Lenovo ブランドのプリインストール・モデルのみ。
診断ディスクの作成	DDIAGS.CMD

右パネルの項目および機能の変更

右パネルの項目を変更するには、pdagui*xx*.ini (ここで、*xx* は言語の指定です) ファイルを編集する必要があります。Rescue and Recovery 環境から pdagui*xx*.ini を取得して、ファイルを置換する方法については、26 ページの『例: pdaguixx.ini』を参照してください。

右パネルの機能リンクのカスタマイズ: 右パネルの上部にあるリンクの機能を変更するには、pdagui*xx*.ini (ここで、*xx* は言語の指定です) の [TitleBar] セクションを変更します。これらのリンクは、左パネルの項目と同じ方法で作動します。ボタン番号値は、00 から 04 です。左パネルと同じアプリケーションを [TitleBar] 項目から起動できます。タイトル・バーから開始できる実行可能ファイルの全リストは、19 ページの『RRUTIL.EXE の使用』を参照してください。

ユーザー・メッセージおよびウィンドウ状況の変更: pdagui*xx*.ini (ここで、*xx* は言語の指定です) には、変更できるユーザーへのメッセージのある次の 2 つのセクションが含まれています。

```
[Welcome window]
```

```
[REBOOT]
```

「ようこそ」ウィンドウは、pdagui*xx*.ini (ここで、*xx* は言語の指定です) の [Welcome] セクションで定義されています。左パネルに対する変更内容に応じて、タイトル行および 01 行目から 12 行目までの情報を変更できます。タイトル、見出し、および太字が表示されるフォントを設定できます。

次の設定は、[Welcome] セクションの例です。

```
[Welcome]
Title = "Rescue and Recovery へようこそ"
Line01 = "Rescue and Recovery(TM) ワークスペースには、Windows(R) 環境に
アクセスできない問題を解決するために役立つ、いくつものツールが用意されています。"
```

```
Line02 = "以下の項目を実行できます。"
Line03 = "* Rescue and Recovery(TM) を使用してファイル、フォルダー、または
バックアップをレスキューおよび復元"
Line05 = "* システム設定およびパスワードを構成"
Line07 = "* インターネットを使用して、サポート・サイトにリンク"
Line09 = "* 診断を使用して問題をトラブルシューティング"
Line11 = "インストール・オプションに応じて機能は変わります。
詳しくは、「Rescue and Recovery」メニューで「概要」をクリックしてください。
Line12 = "注:"
Line13 = "このソフトウェアをご使用いただくと、ご使用条件に合意いただいたことに
なります。ライセンスを表示するには、「Rescue and Recovery」ツールバーで、
「ヘルプ」をクリックし、さらに「ライセンスの表示」をクリックしてください。"
Continue = "続行"
NowShow = "再び表示しない"
NoShowCk =0
WelcomeTitle = "Arial Bold"
WelcomeText = "Arial"
WelcomeBold = "Arial Bold"
```

以下の設定値は、ユーザー・インターフェースにある「タイトル・バー・ヘルプ」機能用です。

- **Command0**

  デフォルトで表示される HTML ベースのヘルプ・ページ。

- **Command1**

  Lenovo ご使用条件 HTML ページ。

- **HELP**

  ヘルプ

- **LICENSE**

  ライセンス

- **CANCEL**

  取り消し

- **Command0**

  %sysdrive%¥Preboot¥Helps¥jp¥f_welcom.htm

- **Command1**

  %sysdrive%¥Preboot¥Helps¥jp¥C_ILA.htm

「ようこそ」ウィンドウを表示しないようにするには、NoShowCk=0 を NoShowCk=1 に変更します。タイトルおよび内容の表示フォントを変更するには、上記の例の最後の 3 行を編集します。

注: 行 14 および 15 は変更または削除しないでください。

pdagui*xx*.ini (ここで、*xx* は言語の指定です) ファイルの [REBOOT] セクションで、以下の行の値を変更できます。

```
NoShowChk=
```

```
RebootText =
```

「NoShowChk」で指定できる値は 0 および 1 です。メッセージを隠すには、チェック・ボックスにマークを付けます。チェック・ボックスにマークを付けると、値は 0 に設定されます。メッセージを表示するには、値を 1 に変更します。

必要に応じて、[REBOOT] セクションのメッセージのフォントを変更できます。たとえば、次のようにして、この値を設定できます。

```
RebootText = "Arial"
```

注: pdagui*xx*.ini (ここで、*xx* は言語の指定です) の [Messages]、[EXITMSG]、および [HelpDlg] セクションは、ファイルで表示できますが、カスタマイズできません。

Opera ブラウザーの設定

Opera ブラウザーには、デフォルト設定ファイルおよびアクティブ設定ファイルの 2 つの設定ファイルがあります。ユーザーはアクティブ設定ファイルを変更することができますが、変更内容は Rescue and Recovery の再起動時に失われます。

ブラウザーの設定に永続的な変更を加えるには、opera6.ini と norm1.ini の両方のコピーを編集します。これらのファイルは %systemdrive% (C:) である C:¥PREBOOT¥OPERA¥PROFILE のフォルダー・パスにあります。opera6.ini の一時的なアクティブ・コピーは RAM ドライブ (Z:) の Z:¥PREBOOT¥OPERA¥PROFILE フォルダーにあります。

注:

1. opera6.ini および norm1.ini ファイルの取得、編集、および配置については、19 ページの『RRUTIL.EXE の使用』を参照してください。
2. Opera ブラウザーは、高度なセキュリティーを保つために一部のブラウザー機能が削除されています。

電子メール

Rescue and Recovery は Opera ブラウザーを介しての Web ベースの電子メールのサポートを提供します。また、大規模な企業のお客様向けの設定を有効にすることができますが、現時点ではサポートしておりません。有効にする方法の参照情報を入手するには、「*システム管理者のハンドブック (System Administrator's Handbook)*」をお読みください。

http://www.opera.com/support/mastering/sysadmin/ (英語のサイトです。)

アドレス・バーの無効化

Opera のアドレス・バーを無効にするには、次の手順を実行します。

1. 19 ページの『RRUTIL.EXE の使用』で説明されている RRUTIL プロセスを使用して、MINIMAL_TOOLBAR(1).INI ファイルを C:¥PREBOOT¥OPERA¥PROFILE¥TOOLBAR から取得します。
2. ファイルを編集モードで開きます。
3. ファイルで [Document Toolbar] セクションを見付けます。
4. ″Address0″ 項目を見付けます。
5. ″Address0″ 項目の前にセミコロン (; コメント区切り記号) を入力します。

注: ここで作業を終了してステップ 7 に進むと Opera ツールバーは無効になりますが、「移動」ボタンとツールバーが機能しないまま表示されています。「移動」ボタンとツールバーを削除するには、ステップ 6 に進んでください。

6. 次の項目を見付けて、それぞれの前にセミコロンを入力します。

```
Button1, 21197=Go Zoom2
```

7. ファイルを保存します。
8. 19 ページの『RRUTIL.EXE の使用』に説明されているように、RRUTIL プロセスを使用してファイルを適用します。 Opera の実行時にアドレス・バーは無効になります。

ブックマークのカスタマイズ

Opera ブラウザーは、この RAM ドライブのファイル Z:¥OPERADEF6.ADR に展開されたブックマークを読み込むように設定されています。このファイルは、Rescue and Recovery の起動時に生成されます。起動時に、自動的に Windows Internet Explorer のブックマークがインポートされ、ブックマークが追加されます。起動時に生成される RAM ドライブのファイルは動的なファイルであるため、Windows 上でブックマークを Internet Explorer に追加すると、Rescue and Recovery ワークスペースの起動時にこれらの項目が自動的にインポートされます。

Internet Explorer のお気に入りの一部またはすべてを除外することができます。特定の Windows ユーザーのお気に入りを除外するには、次のようにします。

1. 19 ページの『RRUTIL.EXE の使用』に説明されているように、RRUTIL プロセスを使用して C:¥PREBOOT¥STARTUP¥OPERA_010.CMD を取得します。
2. ファイルを編集モードで開きます。
3. .CMD ファイルで PYTHON.EXE.FAVS.PYC Z:¥OPERADEF6.ADR という行を見付けます。
4. このコードの行末に、お気に入りを除外する Windows ユーザーの名前を引用符で囲んで入力します。たとえば、すべてのユーザーおよび管理者のお気に入りを除外する場合、次のように入力します。

```
python.exe favs.pyc z:¥Operadef6.adr "All Users, Administrator"
```

5. ファイルを保存します。
6. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

すべての Windows ユーザーの Internet Explorer のお気に入りを Rescue and Recovery 環境で提供されるブラウザーで表示したくない場合、次のステップを実行します。

1. 19 ページの『RRUTIL.EXE の使用』に説明されているように、RRUTIL プロセスを使用して編集するための C:¥PREBOOT¥STARTUP¥OPERA_010.CMD を取得します。
2. ファイルを編集モードで開きます。
3. .CMD ファイルで PYTHON.EXE.FAVS.PYC Z:¥OPERADEF6.ADR という行を見付けます。
4. 以下のいずれかを実行します。
   a. 次のように、行頭に REM と入力します。

   ```
   REM python.exe favs.pyc z:¥Operadef6.adr
   ```

   b. ファイルからコードの行を削除する。

5. ファイルを保存します。
6. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

プロキシー設定の変更

Opera ブラウザーのプロキシー設定を変更するには、次のようにします。

1. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイル C:¥PREBOOT¥OPERA¥PROFILE¥norm1.ini を取得します。
2. ファイルを編集モードで開きます。
3. norm1.ini ファイルの最後に次のセクションを追加します。

   注: [0 or 1] の変数は、チェック項目が有効 (1) または無効 (0) であることを示しています。

```
[Proxy]

Use HTTPS=[0 or 1]

Use FTP=[0 or 1]

Use GOPHER=[0 or 1]

Use WAIS=[0 or 1]

HTTP Server=[HTTP server]

HTTPS Server=[HTTPS server]

FTP Server=[FTP server]

Gopher Server= [Gopher server]

WAIS Server Enable HTTP 1.1 for proxy=[0 or 1]

Use HTTP=[0 or 1]
Use Automatic Proxy Configuration= [0 or 1]
Automatic Proxy Configuration URL= [URL]

No Proxy Servers Check= [0 or 1]

No Proxy Servers =<IP addresses>
```

4. ファイルを保存します。
5. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

HTTP、HTTPS、FTP、Gopher、または WAIS プロキシー・サーバーを追加するには、適切な行の後に `=<address of proxy>` と入力します。たとえば、プロキシー・サーバーのアドレスが http://www.your company.com/proxy である場合、HTTP サーバーの行は次のようになります。

```
HTTP Server=http://www.your company.com/proxy
```

項目にポートを追加する場合、アドレスの後にコロンを入力してから、ポート番号を入力します。″No Proxy Servers″ および ″Automatic Proxy Configuration URL″ も同様です。

```
z:¥preboot¥opera¥profile¥opera6.ini
```

ダウンロード先のパスの有効化または指定

「名前を付けて保存」ウィンドウを表示するには、いくつかの方法があります。ここでは、最も分かりやすい方法を説明します。

1. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、C:¥PREBOOT¥OPERA¥DEFAULTS¥STANDARD_menu.ini ファイルを取得します。
2. 次のストリングを見つけます。

   ```
   ;;Item, 50761
   ```
3. ファイルを編集モードで開きます。
4. [Link Popup Menu] を見つけます。
5. 2 つのセミコロンを削除し、ファイルを保存します。Rescue and Recovery を再起動すると、ユーザーはリンクを右クリックでき、「リンク先を保存」オプションが表示されます。これで、「名前を付けて保存」ウィンドウが表示されるようになります。

   注: 直接のリンク (リダイレクトされるリンクではない) については、上記の手順で機能します。たとえば、リンクの対象が .php スクリプトである場合、Opera はスクリプトのみを保存し、スクリプトがポイントするファイルは保存しません。
6. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

修正ダウンロード・フォルダーを指定するには、次のようにします。

1. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、C:¥PREBOOT¥OPERA¥norm1.ini ファイルを取得します。
2. ファイルを編集モードで開きます。
3. ファイルで、次の行を見付けます。

   ```
   Download Directory=%OpShare%
   ```
4. `%OpShare%` を、ダウンロードするファイルを保存するフォルダーの絶対パスに変更します。
5. norm1.ini ファイルを保存します。Rescue and Recovery ワークスペースを再起動すると、Opera はダウンロードされるファイルを指定されたフォルダーに保存することができるようになります。
6. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

注:

1. ダウンロード先のパスをカスタマイズしても、リンクがリダイレクトされるファイルの場合はターゲット・ファイルを保存できません。
2. Opera ブラウザーは、.zip、.exe、および .txt ファイル・タイプのみをダウンロードし、これらのファイル・タイプについてのみ Opera の動作の変更をカスタマイズするよう設定されています。 Rescue and Recovery ワークスペースでのインターネット・アクセスは、ユーザーの一時的なヘルプを目的として提供されていますので認識されるファイル・タイプの数を限定しています。別のファイル・タイプをダウンロードする必要がある場合、.zip ファイルを作成して、後で解凍してください。
3. ファイル・タイプは、拡張子ではなく、MIME (Multipurpose Internet Mail Extensions) タイプで識別します。たとえば、.txt ファイルに拡張子 .euy の名前を付けても、このファイルは Opera ブラウザーでテキスト・ファイルとして開かれます。

ダウンロード可能なファイル拡張子の追加

Rescue and Recovery ブラウザーでダウンロードできるファイルの拡張子を追加することができます。追加するには、次の手順を実行します。

1. すべての Opera ウィンドウ (Rescue and Recovery ヘルプ・ファイルを含む) が閉じていることを確認します。
2. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、C:¥PREBOOT¥OPERA¥norm1.ini ファイルを取得します。
3. ファイルを編集モードで開きます。
4. ファイルで [File Types] セクションを見付けます。
5. 検索機能を使用して、該当するファイルを見つけてから、以下のいずれかを実行します。
   - 拡張子はあるが、その拡張子のファイルが機能していない場合は、次のステップを実行します。
     a. 拡張子の後の値を 8 から 1 に変更します。 (値 8 は、ブラウザーから該当拡張子のダウンロードを無効にします。値 1 は、ブラウザーから該当拡張子のダウンロードを有効にします。)たとえば、下記のように変更します。

        ```
        video/mgpeg=8,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

        から

        ```
        video/mpeg=1,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

     b. norm1.ini ファイルの [File Types Extension] セクションにあるファイルの mime タイプを検索します。たとえば、VIDEO/MPEG=,8 を検索します。
     c. 値 ,8 を次のように変更します。

        ```
        %opshare%¥,2
        ```

        注: 指定された値がすでに設定されている場合は、値を変更しないでください。

     d. ファイルを保存してから、ファイルを opera6.ini にコピーし、Rescue and Recovery を再起動して変更内容を有効にします。
   - 拡張子が存在せず、該当するタイプのファイル拡張子のダウンロードができない場合は、次のようにします。
     a. norm1.ini の [File Types Extension] セクションで temporary= 項目を見付けます。たとえば、次のような項目です。

        temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|

     b. リストにファイル拡張子を追加します。たとえば、認識される拡張子として .CAB を追加する場合、次のように追加します。

        ```
        temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,cab,|
        ```

        注: 末尾のコンマおよびパイプ記号は、この設定を機能させるために必要です。いずれかが省略されると、リスト内のすべてのファイル拡張子が無効になります。

     c. ファイルを C:¥TEMP¥ に保存します。
     d. ファイルを opera6.ini にコピーします。
     e. Rescue and Recovery ワークスペースを再始動して、変更内容を有効にします。

特定の拡張子を持つファイルの動作の変更

ファイルの動作を変更するには、norm1.ini ファイルの値を置換します。ファイルの動作を拡張子ごとに変更するには、次のようにします。

1. ヘルプ・ファイルを含む、Opera およびすべてのアクティブな Opera ウィンドウを閉じます。
2. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、preboot¥opera¥norm1.ini ファイルを取得します。
3. ファイルを編集モードで開きます。
4. ファイルで [File Types] セクションを見付けます。該当する拡張子を検索します。たとえば、すべての .txt ファイルを SWSHARE フォルダーに保存したいとします。
5. 次の項目を検索します。TEXT/PLAIN=2,,,,TXT,|

   注: 値 2 は、ブラウザーに Opera でテキストとして表示するように設定するものです。値 1 は、ブラウザーにターゲット・ファイルを SWSHARE フォルダーに保存するよう設定しています。
6. .txt の例に続けて、この行を次のように変更します。

   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```
7. ファイルを保存します。
8. 19 ページの『RRUTIL.EXE の使用』内で説明されている RRUTIL プロセスを使用して、ファイルを元に戻します。
9. 変更内容が有効になるように、Rescue and Recovery ワークスペースを再始動します。

固定 IP アドレスの追加

固定 IP アドレスを追加するには、次のステップを実行します。

1. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、¥MININT¥SYSTEM32 winbom.ini ファイルを取得します。
2. ファイルを編集モードで開きます。
3. winbom.ini ファイルの [PnPDriverUpdate] の前に [WinPE.Net] セクションを追加します。次を参考にしてください。

   ```
   [Factory]
   WinBOMType=WinPE
   Reseal=No
   [WinPE]
   Restart=No
   [PnPDriverUpdate]
   [PnPDrivers]
   [NetCards]
   [UpdateInis]
   [FactoryRunOnce]
   [Branding]
   [AppPreInstall]
   ```

   [WinPE.Net] セクションを作成し、以下の行を追加する必要があります。下記の設定はサンプルです。

```
[WinPE.Net]
Gateway=9.44.72.1
IPConfig =9.44.72.36
StartNet=Yes
SubnetMask=255.255.255.128
```

4. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、¥PREBOOT¥SWWORK NETSTART.TBI ファイルを取得します。
5. 下記を、

   ```
   factory -minint
   ```

   から

   ```
   factory -winpe
   ```
6. 以下の行をコメント・アウトします。

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```
7. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、¥SWWORK¥ NETSTART.TBI および ¥MININT¥SYSTEM32 winbom.ini ファイルを元に戻します。

注: デフォルトの環境は DHCP 環境のみをサポートします。

次の表に、IP 構成の項目と説明を示します。

表 7. 固定 IP アドレス項目

項目	説明
Gateway	ゲートウェイの IP アドレスを指定します。デフォルト・ゲートウェイを設定すると、IP ルーティング・テーブルにデフォルトの経路が作成されます。 **構文:** Gateway = *xxx.xxx.xxx.xxx*
IPConfig	Rescue and Recovery ワークスペース起動時にネットワーク接続に使用する IP アドレスを指定します。 **構文:** IPConfig = *xxx.xxx.xxx.xxx*
StartNet	ネットワーク・サービスを開始するかどうかを指定します。 **構文:** StartNet = *Yes* | *No*
SubnetMask	サブネットマスクを 32 ビット値で指定します。 **構文:** SubnetMask = *xxx.xxx.xxx.xxx*

画面の解像度の変更

Rescue and Recovery ワークスペースのデフォルトの解像度 (800 x 600 x 16 ビット) 設定を変更するには、次のようにします。

1. 19 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、¥MININT¥SYSTEM32¥WINBOM.INI ファイルを取得します。
2. ファイルを編集モードで開きます。
3. 次の項目を追加します。

```
[ComputerSettings]
DisplayResolution=800x600x16 or 1024x768x16
```

Rescue and Recovery ワークスペースが起動すると、起動時に「出荷時プリインストール」というタイトルのウィンドウが表示されます。色の数が数万色から 256 色に減ります。

4. 19 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、¥MININT¥SYSTEM32¥WINBOM.INI ファイルを元に戻します。

アプリケーションの開始

Rescue and Recovery ワークスペース環境は、スクリプト、プログラム、またはカスタマイズされたプログラムをサポートする機能を持っています。これらのスクリプトまたはプログラムは、Rescue and Recovery Rescue and Recovery ワークスペース環境がメイン PE インターフェース・ページに到達する前に処理されます。

スクリプトまたはプログラムを配置するフォルダーは ¥Preboot¥Startup です。このフォルダー内のスクリプトまたはプログラムは、英数字で処理されます。たとえば、a.bat と呼ばれるスクリプトは 1.exe よりも前に処理されます。

このフォルダー内にスクリプトまたはプログラムを配置するには、次のステップを実行します。

1. Lenovo Rescue and Recovery 管理ツールのサイト (http://www.ibm.com/jp/pc/think/thinkvantagetech/) から RRUTIL を取得します。
2. 一時フォルダーを作成します。
3. ¥Temp フォルダー内で、以下のフォルダー・ツリーを作成します。
   ¥preboot¥startup
4. スクリプトまたはプログラムを ¥Temp¥preboot¥startup パス内に配置します。
5. コマンド・ラインから RRUTIL 内に、-p ¥Temp を入力します。
6. スクリプトまたはプログラムが正常にコピーされたことを検証するには、RRUTIL 内にコマンド・ラインから -g を入力します。これは、getlist.txt という名前のファイルを生成します。
7. ¥preboot¥startup フォルダーの getlist.txt の内容を調べます。スクリプトまたはプログラムはこのツリーの下にリストされているはずです。

パスワード

以下に、ワークスペースで使用可能な 4 つのパスワード・オプションを示します。

- ワークスペースまたはマスター・パスワード
- ユーザー ID とパスワード、またはパスフレーズ
- バックアップ・パスワード
- パスワードなし

ワークスペースまたはマスター・パスワード

個別のワークスペース・パスワードを設定することができます。このパスワードはコマンド・ライン・インターフェースを介して設定でき、Client Security Solution がインストールされていない場合、唯一使用可能なパスワード・オプションです。

このワークスペース・パスワードは、以下のコマンドを使用して作成できます。
C:¥Program Files¥Lenovo¥Client Security Solution¥pe_setupmasterpwd.exe

このコマンドのパラメーターは以下のとおりです。

表 8.

パラメーター	説明
pe_setupmasterpwd.exe -create password	実際のパスワードを作成します。
pe_setupmasterpwd.exe -verify password	パスワードが有効であり使用できることを確認します。
pe_setupmasterpwd.exe -exists	パスワードが存在するかどうかを確認します。
pe_setupmasterpwd.exe -noenroll	Client Security Solution にユーザーが登録されていない場合でもマスター・パスワードを設定します。
pe_setupmasterpwd.exe -silent	すべてのメッセージを非表示にします。
pe_setupmasterpwd.exe -setmode values	0 = 認証は必要ありません。 1 = ユーザー固有の認証が必要です。 2 = マスター・パスワードが必要です。

ユーザー ID とパスワード、またはパスフレーズ

このオプションは、パスワードまたはパスフレーズ管理に Client Security Solution コードを使用します。ワークスペースの始動時に、Client Security ログオンはユーザーに、このパスワードまたはパスフレーズに対するプロンプトを出します。これは、マルチユーザー環境により良いセキュリティーを提供します。ユーザーが GINA を使用してログオンする場合、そのユーザーはそのユーザーのファイルのみにアクセスが許可され、ほかのユーザーのファイルには許可されません。

このオプションは、Client Security Solution ユーザー・インターフェースによって、または XML スクリプトを介して設定できます。

バックアップ・パスワード

バックアップ・パスワードは、GUI 設定パスワードまたはコマンド・ライン・インターフェース RRCMD を介して、指定されたバックアップを使用して設定できます。以下に例を挙げます。

```
rrcmd backup location=L name=mybackup password=pass
rrcmd basebackup location=L name=basebackup password=pass
rrcmd sysprepbackup location=L name=Sysprep Backup password=pass
```

パスワードなし

このオプションは認証を使用せず、ユーザーはパスワードを使用しないでワークスペースに入ることを許可されます。

パスワード・アクセス

パスワード・アクセスには 3 つのオプションがあります。

- マスター・パスワード

- ユーザー ID とパスワード、またはパスフレーズ
- パスワードなし

マスター・パスワード

マスター・パスワードは、ワークスペースおよびバックアップへのアクセスを許可する単一パスワードです。これはコマンド・ライン・インターフェースを介して設定され、Client Security Solution がインストールされていない場合、唯一のパスワード・オプションです。

ユーザー ID とパスワード、またはパスフレーズ

このオプションは、パスワードまたはパスフレーズ管理に Client Security Solution コードを使用します。ワークスペースの始動時に、Client Security Solution GINA はユーザーに、このパスワードまたはパスフレーズに対するプロンプトを出します。これは、マルチユーザー環境により良いセキュリティーを提供します。ユーザーが GINA を使用してログオンする場合、そのユーザーはそのユーザーのファイルのみにアクセスが許可され、ほかのユーザーのファイルには許可されません。

注: これにはまた、ユーザーの SecureDrive PrivateDisk の暗号化されたボリューム・ファイル内の情報も含まれています。

このオプションは、コマンド・ライン・インターフェースまたは GUI を介して設定できます。

パスワードなし

このオプションは認証を使用せず、ユーザーはパスワードを使用しないでワークスペースに入ることを許可されます。

復元タイプ

以下にファイルを復元するための方法を挙げます。

- ファイルのレスキュー
- 個別ファイルの復元
- オペレーティング・システムおよびアプリケーション
- システムの活性化
- 全体を復元
- 工場出荷時/Image Ultra ビルダー

注: Rescue and Recovery は、復元後にドメイン・ユーザーのキャッシュされたクレデンシャルを取り込むことはできません。

ファイルのレスキュー

ファイルのレスキューは、復元の前にユーザーにバックアップ・ストレージの場所に対するプロンプトを出し、ユーザーがバックアップを選択します。Rescue and Recovery は、現行ユーザーがアクセスを許可されているファイルを表示します。次にユーザーは、レスキューするファイルまたはフォルダー (あるいはその両方) を選択します。システムは、ローカル・ハードディスク以外の、ファイルをレスキュー

するために使用可能なファイルの場所を表示します。ユーザーはレスキューするファイル用に十分なスペースのある宛先を選択し、システムはファイルを復元します。

個別ファイルの復元

個別ファイルの復元はユーザーに、バックアップ・ストレージの場所に対するプロンプトを出し、ユーザーがバックアップを選択します。Rescue and Recovery は、ユーザーがアクセスを許可されているファイルを表示します。次にユーザーは、レスキューするファイルまたはフォルダー (あるいはその両方) を選択し、システムは元の場所へ復元します。

オペレーティング・システムおよびアプリケーション

オペレーティング・システムおよびアプリケーションはユーザーに、システムがファイルを削除する前に、バックアップを選択するオプションを提供します。削除するように指定されたファイルは、レジストリー内の規則によって定義されます。バックアップが選択されると、システムは、選択されたバックアップからレジストリーによって定義されたファイルを復元します。またレジストリー・ファイルには、プログラムを指定できるオプションがあって、復元前、または復元後に実行します。レジストリー設定および値について詳しくは、 145 ページの『付録 B. Rescue and Recovery のカスタマイズ』を参照してください。

注:

1. オペレーティング・システムおよびアプリケーションは常時、パスワードの保存を使用します。
2. オペレーティング・システムおよびアプリケーションの復元は、CD/DVD バックアップからは使用できません。

カスタム・タスクを追加して、バックアップおよび復元の両方の前と後に実行することができます。バックアップおよび復元の設定の詳細については、 145 ページの『付録 B. Rescue and Recovery のカスタマイズ』を参照してください。

システムの活性化

システムの活性化が必要な場合、Rescue and Recovery プログラムは、新規の増分バックアップをとり、ハードディスクをデフラグすることによって、システム・パフォーマンスを最適化します。システムの活性化プロセスは、現在の設定およびデータの保守中に、ウィルス、アドウェアおよびスパイウェアを削除する助けになります。

システムの活性化には、次の手順を実行します。

1. Rescue and Recovery インターフェースから、「**バックアップからシステムを復元する**」アイコンをクリックします。「システムの復元」画面が表示されます。
2. 「システムの復元」画面で、「**システムを活性化します。**」を選択します。
3. 次の手順を実行することによってシステムの活性化を行うために使用する、ドライブとバックアップを選択します。
   a. 使用可能なドライブのドロップダウン・メニューから適切なドライブを選択します。選択したドライブ上でファイルをバックアップして、Rescue and Recovery インターフェースで表示します。

b. システムの活性化のために使用するバックアップ・ファイルを選択します。
c. 「**次へ**」をクリックします。
d. 選択されたバックアップがシステムの活性化のために使用するものであることを確認し、「**次へ**」をクリックして復元処理を開始します。

   注: この操作中は PC を電源オフにしないでください。
e. 「**OK**」をクリックします。進行状況表示バーが表示されます。

カスタム・タスクを追加して、システムの活性化の前か後のいずれかに実行することができます。システムの活性化の設定については、 145 ページの『付録 B. Rescue and Recovery のカスタマイズ』を参照してください。

バックアップの完了

選択されたバックアップが作成されたあとでインストールまたはアンインストールされたアプリケーションは、正しく機能するように再度インストールする必要がある場合があります。バックアップ、復元、活性化、またはアーカイブ手順を開始する前に、システムが AC 電源に接続されていることを確認してください。これを行わないと、データ損失または取り返しの付かないシステム障害という結果になる場合があります。

全体を復元

全体を復元は、ローカル・ドライブ上のすべてのファイルを削除し、選択されたバックアップからファイルを復元します。パスワードの保存が選択された場合、使用可能な最新のパスワードが復元されます。

工場出荷時/Image Ultra ビルダー

工場出荷時/Image Ultra ビルダーは、ハードディスクのデータを消去し、工場出荷時にインストールされたソフトウェアをすべて再インストールします。

パスワードの保存

次の表では、パスワードの保存を使用するかどうかを決定するための考慮事項を示します。

表 9. パスワードの保存の考慮事項

問題	**パスワードの保存を使用した場合の影響**
ユーザーが現行のアカウントおよびパスワードを使用して古いバックアップを復元し、Windows にログインする場合、「暗号化されたファイル・システム」のファイルおよびフォルダーを開くことができない。これらのファイルは元のアカウントおよびパスワードに対して暗号化されており、現行のアカウントおよびパスワードに対しては暗号化されていないため。	• ユーザーは暗号化されたファイル・システムのデータを失う。 • 暗号化されたファイル・システムおよび「パスワードの保存」の併用は不可。

表 9. パスワードの保存の考慮事項 (続き)

問題	パスワードの保存を使用した場合の影響
ユーザーがバックアップ時に終了しない場合、ユーザーのどのユーザー・フォルダーまたはファイルもなくなる。Internet Explorer の「お気に入り」および「アプリケーション」データが存在しない。	• 「ユーザー ID 文書の設定」が設定されない。 • データ損失の可能性がある。
現行アカウントおよびパスワードでユーザー ID を削除すると、すべてのバックアップから削除したユーザー ID の認証情報が削除される。	• ユーザーはデータにアクセスできない。
管理者またはネットワーク管理者が、何人かの元の従業員のアクセスを削除して基本バックアップを復元し、システムをリセットして、全従業員の認証アカウントを削除するため基本バックアップを復元しても、「パスワードの保存」を使用すると元の従業員は従来通りアクセスできる。	• 「Microsoft ユーザー ID」のメンテナンス操作および推奨事項の規格ではない。

ローカルのハードディスクから復元する場合、パスワードの保存が選択されていると、現在のパスワードが使用されます。USB またはネットワークから復元する場合は、最新のバックアップのパスワードが使用されます。

ハードウェア・パスワードのリセット

ハードウェア・パスワードのリセット環境は、Windows とは独立して実行され、これにより、忘れたパワーオンおよびハードディスクのパスワードのリセットが可能になります。登録時に作成している一連の質問に応答することによって、ID が確立されます。このセキュア環境は、パスワードを忘れてしまう前にできるだけ早く作成し、インストールし、登録してください。忘れたハードウェア・パスワードは、登録が完了するまでリセットできません。この回復メディアは、選択された ThinkCentre® および ThinkPad® 上でのみサポートされています。

この環境を作成しても、忘れた Windows パスワード、または Rescue and Recovery ワークスペースと関連したパスワードからのリカバリーの助けにはなりません。この環境を作成することで、そこから忘れたハードウェア・パスワードのリセットが可能な始動デバイス・メニューへ、起動可能なデバイスを追加します。パワーオン・パスワードに対してプロンプトが出されているときに F12 を押すことで、このメニューへアクセスします。

パスワード・デプロイメントのセットアップ関連した 3 つのステージがあります。

1. パッケージ・ビルド
2. パッケージ・デプロイメント
3. 登録

この手順を開始する前に、BIOS 内に管理者またはスーパーバイザー・パスワードを設定します。BIOS 管理者またはスーパーバイザー・パスワード設定がない場合は、環境はセキュアにはなりません。パスワードのリセット・パッケージをデプロイし

ようとするすべてのシステムは、スーパーバイザー・パスワードを持っている必要があります。この手順を完了すると、パワーオン・パスワードとハードディスク・パスワードが同じになります。この手順は、セキュアな環境を作成する助けとなり、またセキュアな環境が作成されたあとで、忘れたパスワードをリセットする助けとなります。

パッケージ・ビルド

セキュア環境を作成するには、次のようにします。

1. ハードウェア・パスワードのリセット・インストールで、「セキュアな環境の作成」を選択して、ハードウェア・パスワードのラジオ・ボタンをリセットします。
2. 「**OK**」をクリックします。「BIOS スーパーバイザー・パスワード」ウィンドウが開きます。
3. 「スーパーバイザー・パスワードの入力」フィールドで、管理者またはスーパーバイザー・パスワードを入力します。このパスワードは、ハードウェア設定を保護するために BIOS にあらかじめ持っている管理者またはスーパーバイザー・パスワードです。
4. 「**OK**」をクリックします。「鍵の作成」ウィンドウが開きます。
5. 鍵の生成領域で、セキュリティー・キーの作成、インポート、またはエクスポートを選択します。このセキュリティー・キーは、ID を認証するために使用されるセキュリティー機能です。セキュリティー・キーを作成する際、以下について検討してください。
   a. この環境を 1 つの PC のためだけに作成する場合は、新規の鍵を生成してください。新規のセキュアなオペレーティング・システムをビルドするたびに、鍵の生成を決定することができます。このオプションには、新しいビルドを作成するたびに、各 PC 上の登録手順を実行することが必要です。同じ鍵が使用される場合は、登録が再実行される必要はありません。同じ鍵が使用される場合は、登録が再実行される必要はありません。
   b. いくつかの PC のためにこの環境を作成する場合は、同じ鍵を使いたいと思うかもしれません。同じ鍵を使用する場合には、セキュアな場所にその鍵を保管する必要があります。
   c. これが鍵を作成する最初の機会であり、この PC だけにセキュアな環境を作成しようとする場合は、「新規の鍵の生成」ラジオ・ボタンを選択します。
   d. これが鍵を作成する最初の機会であり、ほかの PC へデプロイ可能なセキュアな環境を作成したい場合は、「新規の鍵の生成」ラジオ・ボタンを選択します。次に、「鍵をファイルにエクスポート」チェック・ボックスを選択します。「ブラウズ」ボタンを使用して、鍵を保管する場所を定義します。
   e. すでに鍵が作成済みで、ほかの PC へデプロイ可能なセキュアな環境を作成したい場合は、「ファイルから鍵をインポート」ラジオ・ボタンを選択します。「ブラウズ」ボタンを使用して、使用する鍵を配置する場所を定義します。上記のオプションには、作成された鍵が必要です。

   ThinkPad または ThinkCentre および言語ごと (たとえばフランス語、ドイツ語、または日本語) にデプロイするとき、サポートされたシステムの各タイプごとに

ドナー・システムをセットアップします。その目的は、Rescue and Recovery 区画を基にしていて、システムごとに異なるオペレーティング・システムを保証することです。

6. インストール領域で、「ハードウェア・パスワードのリセットを作成したあとで自動的にインストールする」というラベルが付いたフィールドのチェック・ボックスのチェック・マークを外します。
7. 「**OK**」をクリックします。
8. ハードウェア・パスワードのリセット機能がインストール・パッケージが実行されるまでこの PC 上で使用可能にならないことを知らせるダイアログ・ボックスで、「**OK**」をクリックします。

   実行可能ファイルへのパスを検索するには、コマンド・プロンプトで次のように入力します。

   cd %rr%¥rrcd¥passwordreset¥pwdreset.exe

パッケージ・デプロイメント

会社の既存の配布メディアを使用して、作成されたパッケージをデプロイします。

登録

パスワードのリセットを登録するには、次のようにします。

1. pwdreset.exe を実行します。
2. 「**OK**」をクリックして、PC を再起動します。PC は再起動して、BIOS パスワードを入力するようにプロンプトを出します。 BIOS パスワードを入力して、「**Enter**」をクリックします。 PC はセキュアな環境内へ再起動し、「ハードウェア・パスワードのリセットへようこそ」ウィンドウが開きます。
3. これがセキュアな環境を作成する最初の機会であるか、または PC とハードディスクを再登録したい場合は、「ハードウェアのリセットのセットアップ」ラジオ・ボタンを選択します。
4. 「**次へ**」をクリックします。「ハードディスクのセットアップ」ウィンドウが開きます。
5. PC のシリアル番号領域で、セットアップしたい PC の横にある「セットアップ」チェック・ボックスを選択します。
6. 「**次へ**」をクリックします。「新規パワーオン・パスワードを入力」ウィンドウが開きます。
7. 「新規パワーオン・パスワード」フィールドで、使用するパワーオン・パスワードを入力します。すでにパワーオン・パスワードがある場合は、フィールド内に入力したものにリセットされます。さらに、ハードディスクのパスワードも同じパスワードに設定されます。
8. 「**次へ**」をクリックします。「セキュリティーの質問と応答の作成」ウィンドウが開きます。
9. 3 つの質問フィールドのそれぞれで、使用する質問を入力します。
10. 3 つの応答フィールドのそれぞれで、各質問に対する応答を入力します。パワーオン・パスワードを忘れてそれをリセットしようとするイベント内で、各応答を知っていることが必要です。

11. 「**次へ**」をクリックし、それから「**完了**」をクリックします。 PC は Windows 環境内で再起動します。

次に、ハードウェア・パスワードのリセット・インストーラーのエラー・メッセージを挙げます。最初の 2 つは一般タイトルで、メッセージの残りの部分と組み合わせて使用されます。どちらの場合も、製品を再インストールしてください。

- **IDS_STRING_ERR** ″エラー″
- **IDS_STRING_ERR_INT** ″内部エラー″
- **IDS_STRING_ERR_CMDLINE**

  ″入力されたコマンド・ライン・オプションは認識されませんでした。¥n¥nUsage: scinstall [/postenroll | /biosreset | /newplanar]″
- **IDS_STRING_ERR_NOTSUPPORTED**

  ハードウェア・パスワードのリセットはこの PC ではサポートされていません。
- **IDS_STRING_ERR_MEM**

  この PC には、ハードウェア・パスワードのリセット機能を実行するのに十分なメモリーがありません。
- **IDS_STRING_ERR_ENVAR**

  必須の環境変数が失われています。 Rescue and Recovery 3.1 (またはそれ以上) は、ハードウェア・パスワードのリセット機能を使用するためにインストールされている必要があります。
- **IDS_STRING_ERR_MISSINGDLL**

  必須の DLL が失われています。 Rescue and Recovery 3.1 (またはそれ以上) は、ハードウェア・パスワードのリセット機能を使用するためにインストールされている必要があります。
- **IDS_STRING_ERR_BIOSMAILBOX**

  ハードウェア・パスワードのリセットの機能をインストールするための BIOS の更新が失敗しました。 PC の電源を切ってから再起動し、ハードウェア・パスワードのリセットのインストールを再試行してください。
- **IDS_STRING_ERR_INSTALLRETRY**

  この操作は正常に完了しませんでした。再度試行するには、PC の電源を切って再起動し、ハードウェア・パスワードのリセットのインストールを再度実行します。
- **IDS_STRING_ERR_INSTALLPUNT**

  この操作は正常に完了しませんでした。この問題のトラブルシューティングには、システム管理者に相談するか、または詳細について Rescue and Recovery 文書を参照してください。

第 4 章 Client Security Solution のカスタマイズ

Client Security Solution をインストールする前に、Client Security Solution で選択可能なカスタマイズについて理解する必要があります。この章には、Client Security Solution のカスタマイズに関する情報および TPM (Trusted Platform Module) に関する情報が記載されています。この章では、TPM について Trusted Computing Group (TCG) によって定義された用語を使用します。 TPM について詳しくは、次の Web サイトを参照してください。

http://www.trustedcomputinggroup.org/ (英語のサイトです。)

TPM の使用

TPM は、 TPM を利用するソフトウェアにセキュリティー関連の機能を提供するために設計されたエンベデッド・セキュリティー・チップです。エンベデッド・セキュリティー・チップは、システムのマザーボードに搭載され、ハードウェア・バスを介して通信します。 TPM を導入しているシステムは、暗号鍵を作成して暗号化することができ、同じ TPM のみが暗号化を解除することができます。このプロセスは、しばしば鍵のラッピング と呼ばれ、鍵の開示を防止するのに役立ちます。TPM を備えたシステムでは、マスター・ラッピング鍵は、ストレージ・ルート鍵 (SRK) と呼ばれ、 TPM 自体の内部に保管されるので、鍵の秘密 (private) 部分は決して公開されません。エンベデッド・セキュリティー・チップは、他のストレージ・キー、署名鍵、パスワード、およびデータの他の小ユニットも保管できます。TPM には記憶容量の制限があるので、 SRK はチップ外に記憶するその他の鍵の暗号化に使用されます。 SRK はエンベデッド・セキュリティー・チップに残されることは決してないので、保護ストレージの基本になっています。

エンベデッド・セキュリティー・チップの使用は、オプションのプロセスで、Client Security Solution 管理者を必要とします。個人ユーザーでも企業の IT 部門でも、 TPM は初期設定する必要があります。ハードディスク故障からのリカバリーやシステム・ボードの交換など、その後の操作は、Client Security Solution 管理者に限定されます。

Client Security Solution の暗号鍵の管理

Client Security Solution については、2 つの主なデプロイメント・アクティビティーである『所有権の取得』と『ユーザー登録』で説明します。 Client Security Solution セットアップ・ウィザードを初めて実行する際に、所有権の取得プロセスとユーザー登録プロセスが、どちらも初期設定時に実行されます。 Client Security Solution セットアップ・ウィザードを完了した特定の Windows ユーザー ID は、Client Security Solution 管理者で、アクティブ・ユーザーとして登録されます。システムにログインするその他のユーザーは、すべて Client Security Solution に登録するように自動的に要求されます。

- **所有権の取得**

  単一の Windows 管理者のユーザー ID は、唯一の Client Security Solution 管理者としてシステムに割り当てられます。 Client Security Solution の管理機能は、このユーザー ID により実行される必要があります。 TPM の許可は、このユーザーの Windows パスワードか、Client Security パスフレーズのいずれかです。

  注: 忘れてしまった Client Security Solution 管理者パスワードまたはパスフレーズからリカバリーする唯一の方法は、有効な Windows のアクセス権を使用してこのソフトウェアをアンインストールするか、 BIOS 内のセキュリティー・チップをクリアするかのいずれかです。いずれの方法でも、TPM に関連した鍵を介して保護されたデータは、消失します。 Client Security Solution は、忘れてしまったパスワードまたはパスフレーズの自分でリカバリーできるオプション機構も提供します。このため、パスワードまたはパスフレーズは、ユーザー登録機能の一部であるユーザー確認のための質問への応答を基にしています。 Client Security Solution 管理者は、この機能を使用するかしないかを決定します。

- **ユーザー登録**

  所有権の取得プロセスが完了し、 Client Security Solution 管理者が作成されると、ユーザー・ベース鍵 (User Base Key) を作成して、現在ログオンしている Windows ユーザーのクレデンシャルを安全に保管することができます。この設計により、複数のユーザーが Client Security Solution に登録し、単一の TPM を利用することができます。ユーザー鍵は、セキュリティー・チップを介して保護されますが、実際にはチップ外のハードディスクに保管されます。この設計では、セキュリティー・チップに構築された実際のメモリーの代わりに、制限のあるストレージ要素としてハードディスク・スペースを作成します。同じセキュア・ハードウェアを利用できるユーザーの数が飛躍的に増大します。

所有権の取得

Client Security Solution のトラステッド・ルートは、システム・ルート・キー (SRK) です。この移動できない非対称鍵は、 TPM のセキュア環境内に生成され、システムに公開されることは決してありません。この鍵を利用する許可は、Windows 管理者アカウントにより TPM_TakeOwnership コマンドの実行中に得られます。Client Security パスフレーズを利用している場合、Client Security Solution 管理者の Client Security パスフレーズは、TPM 許可になり、それ以外の場合は Client Security Solution 管理者の Windows パスワードになります。

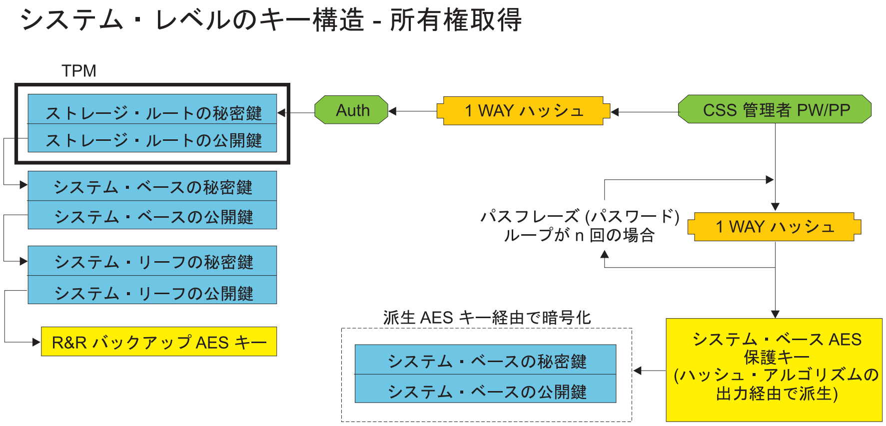


図 1.

システム用に作成された SRK では、その他の鍵ペアは、作成して TPM の外部に保管できますが、ハードウェア・ベースの鍵によってラップまたは保護されます。TPM は SRK を内蔵するハードウェアであり、ハードウェアは損傷することがあるので、システムへの損傷によりデータ・リカバリーが妨げられないようにするためにリカバリー機構が必要です。 図 1 を参照してください。

システムをリカバリーするために、システム・ベース鍵 (System Base Key) が作成されます。この移動可能な非対称ストレージ・キーにより、 Client Security Solution 管理者は、システム・ボード交換や別システムへの計画的移行からリカバリーすることができます。

システム・ベース鍵を保護しながら、通常の操作またはリカバリー時にアクセスできるようにするために、このキーの 2 つのインスタンスが作成され、異なる 2 つの方法によって保護されます。最初に、システム・ベース鍵は、AES 対称鍵を使用して暗号化されます。この鍵は、Client Security Solution 管理者のパスワードまたは Client Security パスフレーズを知っていれば得ることができます。 Client Security Solution リカバリー・キーのこのコピーは、クリアされた TPM またはハードウェア障害により交換されたシステム・ボードからのリカバリー専用です。

Client Security Solution リカバリー・キーの 2 番目のインスタンスは、 SRK によってラップされてキー階層にインポートされます。システム・ベース鍵のこの 2 つのインスタンスにより、 TPM は自身にバインドされた秘密を通常の使用状態で保護することができ、さらに AES 鍵を使用して暗号化されているシステム・ベース鍵を介して、障害のあるシステム・ボードをリカバリーすることができます。AES 鍵は、 Client Security Solution 管理者パスワードまたは Client Security パスフレーズによってアンロックされます。

次に、システム・リーフ鍵 (System Leaf Key) が作成されます。このキーは、バックアップを保護する Rescue and Recovery が使用した AES 鍵など、システム・レベルの機密事項を保護するために作成されます。

ユーザー登録

各ユーザーのデータを同じ TPM によって保護するために、各ユーザーは独自のユーザー・ベース鍵を作成します。この移動可能な非対称ストレージ・キーは、2 回作成され、各ユーザーの Windows パスワードまたは Client Security パスフレーズ

から生成された対称 AES 鍵によって保護されます。次に、ユーザー・ベース鍵の 2 番目のインスタンスは、 TPM にインポートされ、システム SRK によって保護されます。図 2 を参照してください。

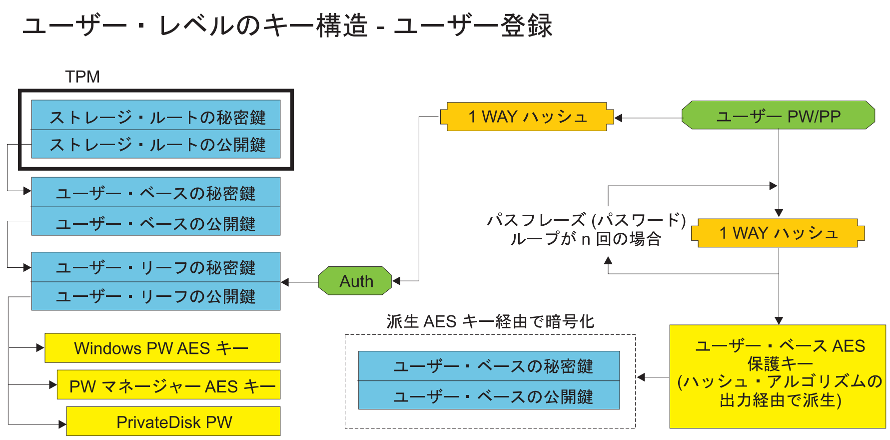


図 2.

作成されたユーザー・ベース鍵では、ユーザー・リーフ鍵 (User Leaf Key) と呼ばれる第 2 非対称鍵が作成されます。ユーザー・リーフ鍵は、インターネット・ログオン情報の保護に使用される Password Manager AES 鍵、データの保護に使用される PrivateDisk パスワード、およびオペレーティング・システムへのアクセスを防護する Windows パスワード AES 鍵など、個別の秘密を保護します。ユーザー・リーフ鍵へのアクセスは、ユーザーの Windows パスワードまたは Client Security Solution パスフレーズによって制御され、ログオン時には自動的にアンロックされます。

ソフトウェア・エミュレーション

システムに TPM が搭載されていない場合は、ソフトウェアをベースにしたトラステッド・ルートが使用されます。ユーザーは同じ機能を使用可能ですが、トラステッド・ルートはソフトウェア・ベースの鍵であるので、セキュリティーは低下します。TPM の SRK は、TPM が提供した保護を行うために、ソフトウェア・ベースの RSA 鍵と AES 鍵で置き換えられます。 RSA 鍵は AES 鍵をラップし、AES 鍵は階層内の次の RSA 鍵の暗号化に使用されます。

システム・ボードの交換

システム・ボードを交換するということは、鍵がバインドされていた旧 SRK がもはや無効になり、別の SRK が必要とされていることが推測されます。これは TPM が BIOS によりクリアされても起こります。

注: システム・ボードの交換は、エミュレーション・モードの使用時は必要ありません。

Client Security Solution 管理者は、システムのクレデンシャルを新規 SRK にバインドすることを要求されます。システム・ベース鍵は、 Client Security Solution 管理者クレデンシャルから得たシステム・ベース AES 保護鍵により暗号化を解除する必要があります。 53 ページの図 3 を参照してください。

注: Client Security Solution 管理者がドメイン・ユーザー ID であり、そのユーザー ID のパスワードが別の PC 上で変更されていた場合、リカバリーを必要とするシステムにログオンするときに最後に使用されたパスワードが、リカバリーのためにシステム・ベース鍵の暗号化を解除するために既知である必要があります。たとえば、デプロイメント中に、 Client Security Solution 管理者のユーザー ID とパスワードが構成されており、このユーザーのパスワードが別の PC 上で変更されている場合は、デプロイメント中に設定された元のパスワードは、このシステムをリカバリーするための必須権限になります。

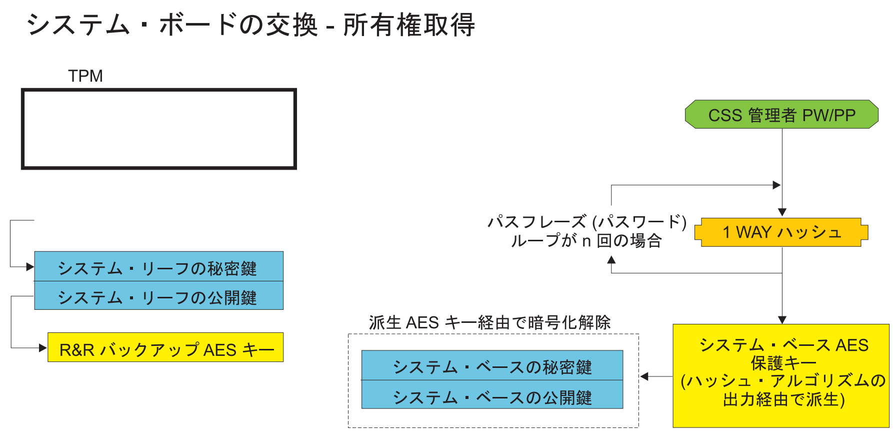


図 3.

以下のステップに従って、システム・ボードの交換を実施してください。

1. Client Security Solution 管理者は、オペレーティング・システムにログオンする。
2. ログオン実行コード (cssplanarswap.exe) は、セキュリティー・チップが使用不可になっていることを認識し、使用可能にするために再起動を要求する (このステップは、BIOS によりセキュリティー・チップを使用可能にすることで回避できます)。
3. システムが再起動され、セキュリティー・チップが使用可能になる。
4. Client Security Solution 管理者がログオンし、次に、新規 Take Ownership プロセスが完了する。
5. システム・ベース鍵は、Client Security Solution 管理者の認証によって得られるシステム基本 AES 保護鍵を使用して暗号化を解除される。システム・ベース鍵は、新規 SRK にインポートされて、システム・リーフ鍵とそれによって保護されているすべてのクレデンシャルを再設定します。
6. これで、システムはリカバリーされます。

各ユーザーがシステムにログオンする度に、ユーザー・ベース鍵がユーザー認証から得られるユーザー・ベース AES 保護鍵により自動的に暗号化を解除され、Client Security Solution 管理者により作成された新規 SRK にインポートされます。 54 ページの図 4 を参照してください。

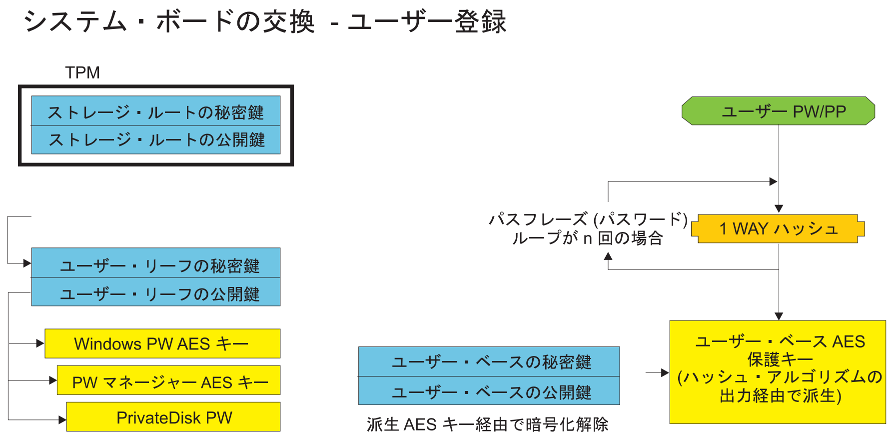


図 4.

XML スキーマの使用

XML スクリプト記述の目的は、IT 管理者が Client Security Solution のデプロイに使用できるカスタム・スクリプトを作成できるようにすることです。 Client Security Solution セットアップ・ウィザードで使用できるすべての機能は、スクリプト記述でも使用可能です。スクリプトは xml_crypt_tool 実行可能モジュールによって保護できます (パスワード (AES 暗号化) を使用または隠ぺいを行う)。いったん作成されると、仮想 PC (vmserver.exe) は、入力としてスクリプトを受け入れます。仮想 PC は、Client Security Solution セットアップ・ウィザードと同一のファンクションを呼び出して、ソフトウェアを構成します。

使用法

すべてのスクリプトは、XML エンコード・タイプ、XML スキーマ、および実行する 1 つ以上の機能を指定する 1 つのタグより構成されています。スキーマは、XML ファイルを検証し、必須パラメーターがそろっていることを確認するために使用されます。スキーマの使用は、現在、推奨されていません。各ファンクションは、ファンクション・タグで囲まれています。各ファンクションには ORDER が含まれています。これは、コマンドが仮想 PC (vmserver.exe) によって実行される順番を指定します。各ファンクションには、バージョン番号も含まれます。現在、すべてのファンクションはバージョン 1.0 です。分かりやすくするために、以下のスクリプト例には、それぞれ 1 つのファンクションのみが含まれています。しかし、実際のスクリプトには複数のファンクションが含まれる可能性が高くなります。Client Security Solution セットアップ・ウィザードを使用すれば、このようなスクリプトを作成できます。 150 ページの『Client Security Solution セットアップ・ウィザード』を参照してください。

注: ドメイン名を必要とするファンクションのいずれかに、パラメーター <DOMAIN_NAME_PARAMETER> が残されている場合は、システムのデフォルトの PC 名が使用されます。

例

以下のコマンドは、XML スキーマの例です。

ENABLE_TPM_FUNCTION

このコマンドは、TPM を使用可能にし、引数 SYSTEM_PAP を使用します。システムに既に BIOS 管理者またはスーパーバイザー・パスワードが設定されている場合は、この引数を指定する必要があります。それ以外の場合、このコマンドはオプションです。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

DISABLE_TPM_FUNCTION

このコマンドは引数 SYSTEM_PAP を使用します。システムに既に BIOS 管理者またはスーパーバイザー・パスワードが設定されている場合は、この引数を指定する必要があります。それ以外の場合、このコマンドはオプションです。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>password</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_ENCRYPT_BACKUPS_FUNCTION

Rescue and Recovery を使用するときは、このコマンドは Client Security Solution を使用したバックアップの保護を使用可能にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

DISABLE_ENCRYPT_BACKUPS_FUNCTION

Rescue and Recovery を使用してバックアップを保護するときは、このコマンドは Client Security Solution を使用したバックアップの保護を使用不可にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>DISABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_PWMGR_FUNCTION

このコマンドは、すべての Client Security Solution ユーザーに対して Password Manager を使用可能にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_CSS_GINA_FUNCTION

このコマンドは、Client Security Solution のログオンを使用可能にします。

```
- <tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_FUNCTION

ThinkVantage 指紋認証ユーティリティーがインストール済みの場合は、このコマンドはログオンを使用可能にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

ThinkVantage 指紋認証ユーティリティーがインストール済みの場合は、ユーザーの簡易切り替え対応のログオンを使用可能にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
     <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

ENABLE_NONE_GINA_FUNCTION

ThinkVantage 指紋認証ユーティリティー、Client Security Solution、または Access Connections などの GINA 関連 TVT コンポーネントのいずれかのログオンが使用可能な場合は、このコマンドは ThinkVantage 指紋認証ユーティリティーと Client Security Solution の両方のログオンを使用不可にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

SET_PP_FLAG_FUNCTION

このコマンドは、Client Security パスフレーズを使用するか、 Windows パスワードを使用するかを決めるために、 Client Security Solution が読み取るフラグを書き込みます。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
         <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
         <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

ENABLE_PRIVATEDISK_PROTECTION_FUNCTION

このコマンドは、SafeGuard PrivateDisk をシステムで使用可能にします。 Safeguard PrivateDisk を使用するためには、各ユーザーを、 ENABLE_PD_USER_FUNCTION によって個別にセットアップする必要があります。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_PRIVATEDISK_PROTECTION_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

SET_ADMIN_USER_FUNCTION

このコマンドは、Client Security Solution の管理者ユーザーを決めるために Client Security Solution が読み取るフラグを書き込みます。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  管理者ユーザーのユーザー名。

- **DOMAIN_NAME_PARAMETER**

  管理者ユーザーのドメイン名。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

ENABLE_PD_USER_FUNCTION

このコマンドは、特定のユーザーが PrivateDisk を使用できるようにします。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  PrivateDisk を使用可能にするユーザーのユーザー名

- **DOMAIN_NAME_PARAMETER**

  PrivateDisk を使用可能にするユーザーのドメイン名

- **PD_VOLUME_SIZE_PARAMETER**

PrivateDisk ボリュームのサイズ (MB)

- **PD_VOLUME_PATH_PARAMETER**

  作成する PrivateDisk ボリュームのパス

- **PD_VOLUME_NAME_PARAMETER**

  作成する PrivateDisk ボリュームの名前。値 PD_USE_DEFAULT_OPTION が指定されている場合は、デフォルト値が自動的に使用されます。

- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  作成する PrivateDisk ボリュームのドライブ名。値 PD_USE_DEFAULT_OPTION が指定されている場合は、デフォルト値が自動的に使用されます。

- **PD_VOLUME_CERT_PARAMETER**

  値 PD_USE_CSS_CERT が渡されると、 PrivateDisk は新規証明書を作成するか、既存の証明書を使用して、それを Client Security Solution 暗号サービス・プロバイダーで保護するかのいずれかを行います。このボリュームのマウントまたはアンマウントは、Client Security Solution パスフレーズまたは Windows パスワードの代わりに暗号サービス・プロバイダーに結合されます。値 PD_USE_DEFAULT_OPTION が指定されている場合は、証明書は使用されず、デフォルトである、ユーザーの Client Security Solution パスフレーズまたは Windows パスワードが使用されます。

- **PD_USER_PASSWORD**

  PrivateDisk ボリュームをマウントまたは作成するために、 Client Security Solution が PrivateDisk を渡すパスワード。値 PD_RANDOM_VOLUME_PWD が指定されている場合は、 Client Security Solution は無作為のボリューム・パスワードを生成します。

- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  このパスワードは、PrivateDisk ボリュームをマウントするための PD_USER_PASSWORD パスワードへのバックアップ用です。Client Security Solution が失敗した場合、この引数に対して渡された値は Client Security Solution から独立しています。値 PD_USE_DEFAULT_OPTION が指定されている場合は、値は使用されません。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_PD_USER_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <PD_VOLUME_SIZE_PARAMETER>500</PD_VOLUME_SIZE_PARAMETER>
          <PD_VOLUME_PATH_PARAMETER>C:¥Documents and Settings¥sabedi¥My Documents¥
             </PD_VOLUME_PATH_PARAMETER>
          <PD_VOLUME_NAME_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_NAME_PARAMETER>
          <PD_VOLUME_DRIVE_LETTER_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_DRIVE
             _LETTER_PARAMETER>
          <PD_VOLUME_CERT_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_CERT_PARAMETER>
          <PD_VOLUME_USER_PASSWORD_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_
```

```
            USER_PASSWORD_
            PARAMETER>
         <PD_USER_PASSWORD>PD_RANDOM_VOLUME_PWD</PD_USER_PASSWORD>
        </FUNCTION>
</CSSFile>
```

INITIALIZE_SYSTEM_FUNCTION

このコマンドは、Client Security Solution システム機能を初期設定します。システム全体の鍵は、このファンクション呼び出しにより生成されます。次のパラメーター・リストで、各ファンクションについて説明します。

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  このパラメーターは、システムの新規所有者パスワードを設定するために使用されます。新規所有者パスワードの場合、このパラメーターの値は現行所有者パスワードにより制御されます。現行所有者パスワードが設定されていない場合、このパラメーターの値が渡されて新規所有者パスワードになります。現行所有者パスワードが既に設定され、管理者が同じ現行の所有者パスワードを使用する場合は、このパラメーターの値が渡されます。管理者が新規所有者パスワードを使用する場合、新規所有者パスワードがこのパラメーターに渡されます。

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  このパラメーターは、システムの現行所有者パスワードです。既にシステムに既存の所有者パスワードがある場合は、このパラメーターは前のパスワードを渡す必要があります。新規所有者パスワードが要求される場合、現行所有者パスワードがこのパラメーターに渡されます。パスワード変更が構成されていない場合は、値 NO_CURRENT_OWNER_AUTH が渡されます。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
        <FUNCTION>
         <ORDER>0001</ORDER>
         <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
         <NEW_OWNER_AUTH_DATA_PARAMETER>pass1word</NEW_OWNER_AUTH_DATA_
             PARAMETER>
         <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT
             _OWNER_AUTH_DATA_PARAMETER>
         <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

このコマンドは、Client Security Solution 管理者権限を変更し、それに応じてシステム鍵を更新します。システム全体の鍵は、このファンクション呼び出しにより再生成されます。パラメーターは次のとおりです。

- NEW_OWNER_AUTH_DATA_PARAMETER

  TPM の新規所有者パスワード

- CURRENT_OWNER_AUTH_DATA_PARAMETER

  TPM の現行所有者パスワード

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>newPassWord</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH
              _DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENROLL_USER_FUNCTION

このコマンドは、Client Security Solution を使用する特定のユーザーを登録します。このファンクションは、ユーザー固有のセキュリティー・キーのすべてを所定のユーザーに作成します。 パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  登録するユーザーのユーザー名

- **DOMAIN_NAME_PARAMETER**

  登録するユーザーのドメイン名

- **USER_AUTH_DATA_PARAMETER**

  ユーザーのセキュリティー・キーを作成するための TPM パスフレーズまたは Windows パスワード

- **WIN_PW_PARAMETER**

  Windows パスワード

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_AUTH_DATA_PARAMETER>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

          <WIN_PW_PARAMETER>myWindowsPassword</WIN_PW_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

このコマンドは、特定の TPM ユーザーのパスワード・リカバリーをセットアップします。 パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  登録するユーザーのユーザー名

- **DOMAIN_NAME_PARAMETER**

  登録するユーザーのドメイン名

- **USER_PW_REC_QUESTION_COUNT**

  ユーザーが応答しなければならない質問の数

- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  特定の質問に対する、保管されている応答。このパラメーターの実名には、応答される質問に対応する番号が連結しています。

- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  質問のすべてが正確に応答されると、ユーザーに示される保管されたパスワード。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test1</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
          <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
         </USER_PW_REC_STORED_PASSWORD_PARAMETER>Pass1word</USER_PW_REC_STORED_PASS
              WORD_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_WIN_PE_LOGON_MODE_FUNCTION

このコマンドは、 Rescue and Recovery ワークスペース環境に入るときに、ユーザー権限を必要とするかどうかを決めるためにプログラムが読み取るフラグを書き込みます。パラメーターは次のとおりです。

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  次の 2 つの有効な選択項目があります。

  – NO_AUTH_REQUIRED_FOR_WIN_PE_LOGON

  – AUTH_REQUIRED_FOR_WIN_PE_LOGON

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_WIN_PE_LOGON_MODE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <WIN_PE_LOGON_MODE_AUTH_PARAMETER>AUTH_REQUIRED_FOR_WIN_PE_LOGON</WIN
```

```
            _PE_LOGON_MODE_AUTH_PARAMETER>
         <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
        </FUNCTION>
</CSSFile>
```

GENERATE_MULTI_FACTOR_DEVICE_FUNCTION

このコマンドは、認証に使用される Client Security Solution の多層デバイスを生成します。パラメーターは次のとおりです。

- USER_NAME_PARAMETER - 管理者のユーザー名。
- DOMAIN_NAME_PARAMETER - 管理者のドメイン名。
- MULTI_FACTOR_DEVICE_USER_AUTH - ユーザーのセキュリティー・キーを作成するための TPM パスフレーズまたは Windows パスワード。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>GENERATE_MULTI_FACTOR_DEVICE_FUNCTION</COMMAND>
<USER_NAME_PARAMETER>myUserName</USER_NAME_PARAMETER>
<DOMAIN_NAME_PARAMETER>domainName</DOMAIN_NAME_PARAMETER>
<MULTI_FACTOR_DEVICE_USER_AUTH>myCssUserPassPhrase</MULTI_FACTOR_DEVICE_USER_AUTH>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

SETUP_PDA_FUNCTION

このコマンドは、Client Security Solution と使用するために Rescue and Recovery ワークスペースをセットアップします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>SETUP_PDA_FUNCTION</COMMAND>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

SET_USER_AUTH_FUNCTION

このコマンドは、Client Security Solution のユーザー認証を設定します。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>SET_USER_AUTH_FUNCTION</COMMAND>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

第 5 章 System Migration Assistant のカスタマイズ

System Migration Assistant をインストールする前に、System Migration Assistant プログラムで選択可能なカスタマイズについて理解する必要があります。次のリストに、System Migration Assistant のカスタマイズ可能な 2 つの部分を示します。

- コマンド・ファイルの編集または変更。
- 追加アプリケーション設定の移行。

注: System Migration Assistant の追加情報については、次の Lenovo Web サイトにある「*System Migration Assistant* デプロイメント・ガイド」を参照してください。

`http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=MIGR-63828`
(英語のサイトです)

コマンド・ファイルの作成

取り込みフェーズで、System Migration Assistant はコマンド・ファイルとアーカイブ設定の内容を読み取ります。このセクションでは、コマンド・ファイルおよびその中に指定できるステートメントについて説明します。

System Migration Assistant にはデフォルトのコマンド・ファイル (command.xml) があり、このファイルをテンプレートとして使用して、コマンド・ファイルをカスタマイズすることができます。System Migration Assistant をデフォルトの場所にインストールした場合、このファイルは d:¥%RR%¥migration¥bin ディレクトリーにあります。

注: System Migration Assistant 5.1 では、XML テクノロジーを使用して、コマンド・ファイル内のコマンドを記述します。

System Migration Assistant 5.1 コマンド・ファイルについては、以下の点を考慮に入れてください。

- XML コマンド・ファイルは Unicode (UTF-16) フォーマットで保管する必要があります。
- コマンド・ファイルは XML バージョン 1.0 構文に準拠し、大文字と小文字を区別します。
- 各コマンドおよびパラメーター・セクションは、必ず <TagName> で始まり、</TagName> で終わり、これらのタグの間でその値について記述する必要があります。
- 構文エラーがあると、System Migration Assistant の実行時にエラーになります。System Migration Assistant にエラーが発生すると、System Migration Assistant はエラーをログ・ファイルに書き込んで操作を実行します。エラーの重大度により、最終結果が破壊される可能性があります。

ファイル・コマンド

次の表は、コマンド・ファイルに使用できるコマンドを示したものです (ただし、ファイルの移行とレジストリーに関するコマンドを除きます)。

表 10.

コマンド	パラメーター	パラメーター値と例
<Desktop>	• <accessibility> • <active_desktop> • <colors> • <desktop_icons> • <display> • <icon_metrics> • <keyboard> • <mouse> • <pattern> • <screen_saver> • <sento_menu> • <shell> • <sound> • <start_menu> • <taskbar> • <wallpaper> • <window_metrics> • <desktop_settings> • <time_zone>	デスクトップ設定を選択するには、このパラメーターを「True」に設定します。それ以外の場合は、パラメーターを「False」に設定するか、指定解除しておきます。 例: `<Desktop>` `<colors>true</colors>` `<desktop_icons>true</desktop_icons>` `<screen_saver>true</screen_saver>` `<start_menu>false</start_menu>` `<time_zone>true</time_zone>` `</Desktop>`
<Network>	• <ip_subnet_gateway_configuration> • <dns_configuration> • <wins_configuration> • <computer_name> • <computer_description> • <domain_workgroup> • <mapped_drives> • <shared_folders_drives> • <dialup_networking> • <odbc_datasources>	デスクトップ設定を選択するには、このパラメーターを「True」に設定します。それ以外の場合は、パラメーターを「False」に設定するか、指定解除しておきます。 例: `<Network>` `<computer_name>true<computer_name>` `<mapped_drives>false</mapped_drives>` `</Network>`

表 10. (続き)

コマンド	パラメーター	パラメーター値と例
<Applications>	<Application> サポートされているアプリケーションの全リストは、http://www.ibm.com/jp/pc/think/thinkvantagetech/ にある「*ThinkVantage System Migration Assistant* ユーザーズ・ガイド」を参照してください。	例: サポートされるすべてのアプリケーションを取り込むには、$(all) を設定します。 `<Applications>` `<Application>Lotus Notes</Application>` `<Application>Microsoft Office</Application>` `<//Applications>` または `<Applications>` `<Application>$(all)</Applications>`
<Registries>	• <Registry> • <hive> • <keyname> • <value>	レジストリー設定の取り込みまたは適用を行うには、コマンド・ファイルのパラメーターとして hive、keyname および value を指定します。 例: <HKEY_CURRENT_USER><Control Panel><Colors><Menu Bar><236.233.218>
<IncUsers>	<UserName>	すべてのユーザー・プロファイルを取り込むには、「$(all)」を設定するか、すべてのユーザーを表すワイルドカード文字として「*¥*」を使用します。それ以外の場合は、ユーザーを個別に指定します。 次のワイルドカードが使用可能です。 • *¥* は可変長のワイルドカード用です。 • % は固定長のワイルドカード (1 文字) 用です。 例: `<IncUsers>` `<UserName>Administrator</UserName>` `<UserName>domain¥Jim</UserName>` `</IncUsers>`
<ExcUsers>	<UserName>	移行処理からユーザーを除外するには、ユーザーのドメインおよびユーザー名を指定します。 次のワイルドカードが使用可能です。 • * は可変長のワイルドカード用です。 • % は固定長のワイルドカード (1 文字) 用です。

表 10. (続き)

<table>
<tr><th>コマンド</th><th>パラメーター</th><th>パラメーター値と例</th></tr>
<tr><td><Printers></td><td><Printer>

<PrinterName></td><td>この制御ステートメントは、ソース PC とターゲット PC の両方で有効です。

すべてのプリンターを取り込むには、このパラメーターを $(all)</i> に設定します。デフォルト・プリンターのみを取り込む場合は、各プリンターを個別に指定します。パラメーターを <i>$(DefaultPrinter) に設定します。

例:

<pre><Printers>
  <Printer>$(all)</Printer>
</Printers></pre>
または

<pre><Printers>
  <Printer>
   <PrinterName>Lenovo 5589-L36</PrinterName>
  </Printer>
</Printers></pre>
または

<pre><Printers>
  <Printer>$(DefaultPrinter)</Printer>
</Printers></pre></td></tr>
</table>

表 10. (続き)

コマンド	パラメーター	パラメーター値と例
<MISC>	<bypass_registry>	レジストリー設定の選択をすべて解除するには、「True」に設定します。それ以外の場合は、「False」に設定するか、指定解除しておきます。
	<overwrite existing files>	既存のファイルを上書きするには、「True」に設定します。それ以外の場合は、「False」に設定するか、指定解除しておきます。
	<log_file_location>	System Migration Assistant でログ・ファイルの書き込み先となるディレクトリーを指定するには、完全修飾ディレクトリー名を入力します。他のシステムの共用ディレクトリーを指定できます。 このパラメーターを設定しない場合、System Migration Assistant はログ・ファイルを d:/InstDir/ に書き込みます。ここで、d はハードディスクのドライブ名、 /InstDir/ は System Migration Assistant のインストール先ディレクトリーです。
	<temp_file_location>	System Migration Assistant が一時ファイルを書き込むディレクトリーを指定するには、完全修飾ディレクトリー名を入力します。他のシステムの共用ディレクトリーを指定できます。 このパラメーターを設定しない場合、System Migration Assistant は一時ファイルを d:/InstDir/etc/data に書き込みます。ここで、d はハードディスクのドライブ名、 /InstDir/ は System Migration Assistant のインストール先ディレクトリーです。
	<resolve_icon_links>	アクティブ・リンクが設定されたアイコンのみをコピーするには、「True」に設定します。それ以外の場合は、パラメーターを「False」に設定するか、指定解除しておきます。

ファイル移行コマンド

System Migration Assistant はファイル移行コマンドの処理を次の順序で処理します。最初にファイル組み込みコマンドが実行され、次にファイル除外コマンドがその組み込みファイルから実行されます。

System Migration Assistant は、ソース PC 上のファイルとフォルダーの元の場所に応じて、ファイルを選択および選択解除します。ファイル・リダイレクト・ステートメントはプロファイルに保存され、適用フェーズで解釈されます。ファイル移行は、サブディレクトリーで再帰的に用いられます。

ファイル名とディレクトリー名の処理では、大文字と小文字は区別されません。

次表では、ファイル移行コマンドについて説明します。すべてのファイル移行コマンドはオプションです。

表 11.

コマンド	パラメーター	説明	例
<FilesAndFolders>	<run>	コマンドの処理を開始します。 </run> パラメーターは、コマンドの処理を終了します。	ファイル移行の取り込みまたは適用を行うには、このパラメーターを「True」に設定します。それ以外の場合は、パラメーターを「False」に設定するか、指定解除しておきます。 例: `<FilesAndFolders>` `<run>true</run>` `</FilesAndFolders>`
<Exclude_drives>	<Drive>	スキャンからドライブを除外するためにドライブ名を指定します。	例: `<ExcludeDrives>` `<Drive>D</Drive>` `<Drive>E</Drive>` `</ExcludeDrive>`
<Inclusions>	<IncDescription> <Description> <DateCompare> <Operand> <Date>	• <Description> は完全修飾ファイル名です。ファイル名とフォルダー名の両方にワイルドカード文字を使用できます。 • <DateCompare> は、作成日に基づいてファイルを選択するためのオプション・パラメーターです。 – <Operand> は NEWER または OLDER のいずれかです。 – <Date> は基本となる日付で、mm/dd/yyyy 形式で表します。	指定されたディレクトリーに入っているすべての一致ファイルを検索します。 例: 例 1 `<Inclusions>` `<IncDescription>` `<Description>` `c:¥MyWorkFolder¥ls` `</Description>` `</IncDescription>` `</Inclusions>` **注:** フォルダー名を指定するには、記述の最後に .¥. を付加します。

表 11. (続き)

コマンド	パラメーター	説明	例
<Inclusions>	<SizeCompare> <Operand> <Size> <Dest> <Operation> ここで、	• <SizeCompare> は、サイズに基づいてファイルを指定するためのオプション・パラメーターです。 – <Operand> は LARGER または SMALLER のいずれかです。 – <Size> は MB 単位でのファイル・サイズです。 • <Dest> は、ターゲット・システム上の、ファイルが書き込まれる宛先フォルダーの名前を指定するオプション・パラメーターです。 • <Operation> は、ファイル・パスの処理方法を指定するオプション・パラメーターです。以下のいずれかを指定します。 – P - ファイルのパスを保存し、<Dest> パラメーターで指定された場所から始まるターゲット・システムにファイルを再作成します。 – R - ファイルのパスを削除し、<Dest> パラメーターで指定された場所にファイルを直接入れます。 **注:** <Operation> タグで P または R コマンドが使用されない場合、デフォルトで <Operation> は空のまま残されます。たとえば、<Operation></Operation> のようになります。	例 2 <Inclusions> <IncDescription> <Descriptin>C:¥MyWorkFolder¥*.* </Decsription> <DateCompare> <Operand>NEWER</Operand> <Date>07/31/2005</Date> </DateCompare> </IncDescription> </Inclusions> 例 3 <Inclusions> <IncDescription> <Description>C:¥MyWorkFolder/*.* </Description> <SizeCompare> <Operand>SMALLER</Operand> <Size>200</Size> </SizeCompare> </IncDescription> </Inclusions> 例 4 <Inclusions> <IncDescription> <Description>C:¥MyWorkFolder¥*.* </Description> <Dest>D:¥MyNewWorkFolder</Dest> <Operation> </Operation> <IncDescription> </Inclusions>

表 11. (続き)

コマンド	パラメーター	説明	例
<Exclusions>	<ExcDescription> <Description> <DateCompare> <Operand> <Date> <SizeCompare> <Operand> <Size> ここで、	• <Source> は、完全修飾ファイル名またはフォルダー名です。ファイル名とフォルダー名の両方にワイルドカード文字を含めることができます。 • <DateCompare> は、作成日に基づいてファイルを選択するためのオプション・コマンドです。 – <Operand> は NEWER または OLDER のいずれかです。 – <Date> は基本となる日付で、mm/dd/yyyy 形式で表します。 • <SizeCompare> は、サイズに基づいてファイルを選択するためのオプション・パラメーターです。 – <Operand> は LARGER または SMALLER のいずれかです。 – <Size> は MB 単位でのファイル・サイズです。	指定されたディレクトリーに入っているすべての一致ファイルを選択解除します。 例: 例 1 `<Exclusions>` `<ExcDescription>` `<Description>C:¥YourWorkFolder` `</Description>` `</ExDescription>  </Exclusions>` 例 2 `<Exclusions>` `<ExcDescription>` `<Description>C:¥YourWorkFolder` `</Description>` `<DateCompare>` `<Operand>OLDER</Operand>` `<Date>07/31/2005</Date>` `</DateCompare>` `</ExcDescription>` `</Exclusions>` 例 3 `<Exclusions>` `<ExcDescription>` `<Description>C:¥YourWorkFolder` `</Description>` `<SizeCompare>` `<Operand>LARGER</Operand>` `<Size>200</Size></SizeCompare>` `</ExcDescription>` `</Exclusions>`

ファイル移行コマンドの例

このセクションは、ファイル移行コマンドの例を含みます。これらの例は、ファイル選択を絞り込むために、ファイル組み込みコマンドとファイル除外コマンドを結合する方法を示しています。コマンド・ファイルのファイル処理セクションのみを示します。

取り込みフェーズでのファイルの選択

このセクションは、取り込みフェーズでファイル選択のために使用する 3 つのコード例を示します。

例 1

次のコード例では、.doc 拡張子 (Microsoft Word 文書) のすべてのファイルを選択し、それらのファイルを「d:¥My Documents」ディレクトリーに再配置します。次に、d:¥No_Longer_Used ディレクトリーに入っているすべてのファイルを除外します。

```
<Inclusions>
<IncDescription>
<Description>*:¥*.doc/s</Description>
<Dest>d:¥My Documents</Dest>
<Operation>r</Operation>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:¥No_Longer_Used¥</Description>
</ExcDescription>
</Exclusions>
```

例 2

次のコード例では、d ドライブの内容を選択し、 d ドライブのルートにあるすべてのファイルと .tmp 拡張子のすべてのファイルを除外します。

```
<Inclusions>
<IncDescription>
<Description<d:¥*.*/s<¥Description>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:¥*.*</Description>
</ExcDescription>
<ExcDescription>
<Description>*:¥*.tmp/s</Description>
</ExcDescription>
</Exclusions>
```

例 3

次のコード例では、c ドライブの内容全体を選択し、ディレクトリー %windir% にあるすべてのファイルを除外します。%windir% ディレクトリーは、Windows ディレクトリーを指定します。

```
<Inclusions>
<IncDescription>C:¥*.*/s</Description>
</Inclusion>
<Exclusions>
<ExcDescription>
<Description>%windir%¥</Description>
</ExcDescription>
</Exclusions>
```

例 4

次のコード例では、現行ログオン・ユーザーのユーザー・プロファイル・パスである %USERPROFILE% フォルダーの内容全体を選択し、 .dat 拡張子で、「Local Settings」サブフォルダーにあるすべてのファイルを除外します。

```
<Inclusions>
<IncDescription>
<Description>%USERPROFILE%¥</Description>
</IncDescription>
</Inclusions>
<Exclusions>
```

追加アプリケーション設定の移行

カスタム・アプリケーション・ファイルを作成する場合は、カスタマイズされた設定のストレージ・ロケーションを含め、アプリケーションについて完全な知識を持っている必要があります。デフォルトでは、いくつかのアプリケーションの設定を移行するように System Migration Assistant が事前構成されています。System Migration Assistant でサポートされるアプリケーションのリストは、Lenovo Web サイト
http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=MIGR-50889&style=lenovo (英語のサイトです) を参照してください。また、カスタム・アプリケーション・ファイルを作成して追加アプリケーションの設定を移行することもできます。

このファイルは、application.xml または application.smaapp という名前で、d:¥%RR%¥Migration¥bin¥Apps に配置されている必要あります。ここで、*Apps* はアプリケーションを示し、 d はハードディスクのドライブ名です。同一アプリケーションの application.smaapp ファイルと application.xml カスタム・アプリケーション・ファイルの両方が存在する場合、application.smaapp ファイルが優先されます。

新規アプリケーションをサポートするために、既存のアプリケーション・ファイルをコピーして必要な変更を行うこともできます。たとえば、 Microsoft_Access.xml は既存のアプリケーション・ファイルです。

アプリケーション・ファイルについては、以下の点を考慮してください。

- *application*.xml
  - デフォルトでは、System Migration Assistant がインストールされているときは、 application.xml のみが存在します。
  - 「<!--」と「-->」で囲まれた <タグ> は、コメントとして扱われます。例:

```
<!--Files_From_Folders>
<!-Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.* /s
</Files_From_Folder>
 <Files_From_Folder>%Personal Directory%¥*.pdf</Files_from_Folder>
</Files_From_folders-->
```

  - 各コマンドは別々のセクションで記述する必要があります。
  - 各セクションは、<AppInfo> や <Install_Directories> などのタグで囲まれたコマンドで始まります。 1 つのセクションに 1 つ以上のフィールドを入力できますが、各フィールドは別々の行に分かれている必要があります。
  - アプリケーション・ファイルに構文エラーが含まれている場合、 System Migration Assistant の操作は続行され、エラーがログ・ファイルに書き込まれます。

表 12 は、アプリケーション・ファイルについての情報を示します。

表 12.

セクション	**コマンド**	**値**	**作業の内容**
<Applications>			
	<Family>	文字列。先行スペースは無視されます。文字列を引用符で囲まないでください。	アプリケーションのバージョンに依存しない固有名を指定します。System Migration Assistant をバッチ・モードで実行する場合は、このストリングをコマンド・ファイルのアプリケーション・セクションで使用します。 例: `<Family>adobe Acrobat Reader</Family>`
	<SMA_Version>	数値。	System Migration Assistant のバージョン番号を指定します。 以下に例を示します。 `<SMA_Version>SMA 5.0</SMA_Version`
	<App>	*ShortName*。ShortName はアプリケーションのバージョン固有のショート・ネームです。	1 つ以上のアプリケーションのバージョン固有のショート・ネームを指定します。 以下に例を示します。 `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*ShortName*>。ここで、*ShortName* は「Applications」セクションで指定したアプリケーションのショート・ネームです。			
	<Name>	文字列	アプリケーションの名前を指定します。
	<Version>	数値	アプリケーションのバージョンを指定します。
	<Detects> <Detect>	*Root, PathAndKey*	レジストリー・キーを指定します。System Migration Assistant は、指定されたレジストリー・キーを検索してアプリケーションを検出します。 以下に例を示します。 `<Detects>` `<Detect>` `<hive>HKLM</hive>` `<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥</keyname>` `</Detect>` `</Detects>`

<Install_Directories> 例: `<Install_Directories>` `<Install_Directory>` `<OS>WinXP</OS>` `<Registry>` `<hive>HKLM</hive>` `<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>` `<value>(Default)</value>` `</Registry>` `</Install_Directory>` `<Install_Directory>` `<OS>Win2000</OS>` `<Registry>` `<hive>HKLM</hive>` `<keyname>Software¥adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>` `<value>(Default)</value>` `</Registry>` `</Install_Directory>` `</Install_Directories>`

	<OS>	文字列	オペレーティング・システムを指定し、以下のいずれかを指定できます。 • Windows XP • Windows 2000 • Windows NT • Windows 98
	<Registry>	*hive* は、HKLM または HKCU のいずれかです。 *keyname* はキー名です。 *value* は、移行するレジストリー値を指定するオプション・コマンドです。	レジストリーに現れるインストール・ディレクトリーを指定します。アプリケーションのインストール・ディレクトリーを示すレジストリーも指定します。

	SMAVariable¥Location[|File][/s] ここで、 • SMAvariable は、カスタマイズ・ファイルの場所を指定する次のいずれかの変数です。 – %Windows Directory% (オペレーティング・システム・ファイルの場所) – %Install Directory% (Install_Directories セクションで定義されたアプリケーションの場所) – %Appdata Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Application Data ディレクトリー) – %LocalAppdata Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Local Settings フォルダーの Application Data ディレクトリー) – %Cookies Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Cookies ディレクトリー) – %Favorites Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Favorites ディレクトリー) – %Personal Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリー (My Documents) である Personal ディレクトリー。この環境変数は、Windows NT4 では使用できません。)	移行したいカスタマイズ・ファイルを指定します。 例: `<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi</Files_And_Folders>` %AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが System Migration Assistant で取り込まれます。サブディレクトリー内のファイルは含まれません。 `<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥ /s</Files_From_Folder>` %AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが System Migration Assistant で取り込まれます。サブディレクトリー内のファイルも含まれます。 `<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.*</Files_From_Folder>` %AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが System Migration Assistant で取り込まれます。サブディレクトリー内のファイルは含まれません。 `<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.* /s</Files_From_Folder>` %AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが System Migration Assistant で取り込まれます。サブディレクトリー内のファイルも含まれます。 `<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi</Files_From_Folder>` 「Whapi」の後ろに「¥」がない場合、 System Migration Assistant では「Whapi」はフォルダーではなくファイルとして扱われます。

	• *Location* は、完全修飾のファイルまたはディレクトリーを指定します。ワイルドカード文字は、ファイル名には使用できますが、パスには使用できません。 ディレクトリーを指定すると、すべてのファイルがコピーされます。 • *[File]* は、オプション・パラメーターで、 Location がディレクトリーを指定し、File がコピー対象のファイルである場合にのみ使用できます。ワイルドカード文字は、ファイル名には使用できますが、パスには使用できません。 • *[/s]* はオプション・パラメーターです。 [/s] を使用すると、サブディレクトリー内のすべてのファイルがコピーされます。 • SMA5.0 ユーザーは、 Windows 環境変数を使用できます。 SMA を開始したユーザーの環境変数は、Windows 環境変数の値として使用されます。	
<Registries> オプション		
	hive は、HKLM または HKCU のいずれかです。 *keyname* はキー名です。value は、移行するレジストリー値を指定するオプション・コマンドです。	移行したいレジストリーを指定します。 例: `<Registries>` `<Registry>` `<hive>HKCU</hive>` `<keyname>Software¥Adobe¥Acrobat</keyname>` `<value></value>` `</Registry>` `</Registries>`
<Registry_Excludes> オプション		
	hive は、HKLM または HKCU のいずれかです。 *keyname* はキー名です。value は、移行するレジストリー値を指定するオプション・コマンドです。	選択したレジストリーから除外したいレジストリー・キーと値を指定します。 例: `<Registry_Excludes>` `<Registry>` `<hive>HKCU</hive>` `<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer` `</keyname>` `<value>xRes</value>` `</Registry>` `</Registry_Excludes>`
<Files_Through_Registry>		

	<OS> は、オペレーティング・システムを指定し、以下のいずれかの値です。 • WinXP • Win2000 • WinNT • Win98 <Registry> は、レジストリー項目を指定し、 hive、keyname、value のフォーマットになっています。ここで、 • hive は、HKLM または HKCU のいずれかです。 • keyname はキー名です。 • value は、移行するレジストリー値を指定するオプション・コマンドです。 File はファイル名です。ワイルドカード文字を使用できます。 File はファイル名です。ワイルドカード文字を使用できます。	移行するカスタマイズ・ファイルを指定します。 例: <Files_Through_Registries> <Files_Through_Registry> <OS>WinXP</OS> <Registry> <hive>HKCU</hive> <keyname>Software¥Lotus¥Organizer¥99.0¥Paths</keyname> <value>Backup</value> </Registry> <File>*.*/s</File> </Files_Through_Registry> </Files_Through_Registries>
<Files_From_Folders> オプション		
<PreTargetBatchProcessing>		
	<PreTargetBatchProcessing> <!CDAT[batch commands]] <PreTargetBatchProcessing>	<PreTargetBatchProcessing> は、適用フェーズで <Registries> が処理される前にバッチ処理を実行します。 例: <PreTargetBatchProcessing> <!CDATA[copy /y c:¥temp¥*.* c:¥migration del c:¥migration¥*.mp3 </PreTargetBatchProcessing>
<TargetBatchProcessing>		
	<TargetBatchProcessing> <!CDAT[batch commands]] <TargetBatchProcessing>	<TargetBatchProcessing> は、適用フェーズで <Registries> が処理された後にバッチ処理を実行します。 例: <TargetBatchProcessing> <!CDATA[copy /y c:¥temp¥*.* c:¥migration del c:¥migration¥*.mp3 <TargetBatchProcessing>

アプリケーション・ファイルの作成

カスタム・アプリケーション・ファイル用にどのアプリケーション設定を移行する必要があるかを決定するには、アプリケーションを慎重にテストしなければなりません。

アプリケーション・ファイルを作成するには、以下のステップを完了します。

1. Unicode を処理できるテキスト・エディターを使用して既存の application.xml ファイルを開きます。SMA をデフォルトの場所にインストールした場合、application.xml ファイルは、d:¥%RR%¥Migration¥bin¥Apps ディレクトリーに入れられます。ここで、d はハードディスクのドライブ名です。
2. 移行したいアプリケーションとアプリケーション設定についてこの application.xml ファイルを変更します。
3. <Applications> セクションの情報を変更します。
4. <Application Shortname=*Shortname*> セクションの <Name> コマンドと <Version> コマンドを変更します。
5. 移行する必要があるレジストリー・キーを決定します。
   a. 「**スタート**」をクリックしてから、「**ファイル名を指定して実行**」をクリックします。「ファイル名を指定して実行」ウィンドウが開きます。「名前」フィールドに regedit と入力して、「**OK**」をクリックします。「レジストリ エディタ」ウィンドウが開きます。
   b. 左側のペインで「**HKEY_LOCAL_MACHINE**」ノードを展開します。
   c. 「**Software**」ノードを展開します。
   d. ベンダー固有のノード (たとえば、「**Adobe**」) を展開します。
   e. アプリケーションのレジストリー・キーが見つかるまで、調査を続行します。この例では、レジストリー・キーは SOFTWARE¥Adobe¥Acrobat Reader¥6.0 です。
   f. 「Detect」フィールドの値を設定します。例:

```
<Detects>
<Detect
<hive>HKLM</hive>
<keyname>Software¥Adobe|acrobat Reader¥6.0<keyname>
</Detect
</Detects
```

6. Install_Directories セクションの Name コマンドと Version コマンドを変更します。
7. アプリケーションのインストール・ディレクトリーへのパスを確認します。
   a. 「レジストリ エディタ」ウィンドウから、HKLM¥SOFTWARE¥Adobe¥Acrobat Reader¥6.0¥InstallPath ノードにナビゲートします。
   b. 該当するコマンドをアプリケーション・ファイルの Install_Directories セクションに追加します。例:

```
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

   注: アプリケーション固有のディレクトリーが HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥AppPaths ディレクトリーにない場合は、HKLM¥Software ツリー内の他の場所で、インストール・パスを含むディレクトリーを見つける必要があります。ディレクトリーを見つけたら、そのキーを <Install_Directories> セクションで使用します。

8. <Files_From Folders> セクションで、移行したいカスタマイズ・ファイルを指定します。
   a. 多くのアプリケーションは、デフォルトで、ファイルを Documents and Settings サブディレクトリーに保存しているので、Application Data ディレクトリーでこのアプリケーションに関連するディレクトリーを調べてください。 それが存在している場合は、次のコマンドを使用してそのディレクトリーとファイルを移行することができます。

      ```
      <Files_From_Folder>SMAvariable¥Location¥[File] [/s] </Files_From_Folder>
      ```

      ここで、Location¥ は完全修飾ファイルまたはディレクトリー、 [File] は、Location¥ がディレクトリーを指定する場合に限り使用可能なオプション・パラメーターです。 Adobe Reader の例では、カスタマイズ・ファイルは Preferences ディレクトリーに入っています。
   b. 個人用設定が保存されている可能性があるすべての関連ディレクトリーを調べます。
   c. Local Settings ディレクトリーを調べます。
9. 移行したいレジストリー項目を決定します。それらは HKCU (HKEY_CURRENT_USER) に入っています。アプリケーション・ファイルの <Registries> セクションで、該当するコマンドを追加します。
10. application.xml ファイルを c:¥program files¥lenovo¥Rescue and Recovery¥Migration¥bin¥apps ディレクトリーに保存します。ここで、c はハードディスクのドライブ名です。
11. 新規のアプリケーション・ファイルをテストします。

Adobe Reader 用の application.xml ファイルの例

このセクションでは、Adobe Reader のアプリケーション・ファイルを紹介します。

```
<?xml version="1.0"?>
<Applications>
<Family>Adobe Acrobat Reader</Family>
<SMA_Version>SMA 5.0</SMA_Version>
<APP>Acrobat_Reader_70</APP>
<APP>Acrobat_Reader_60</APP>
<APP>Acrobat_Reader_50</APP>
<Application ShortName="Acrobat_Reader_50">
<AppInfo>
<Name>Acrobat_Reader_50</Name>
<Version>5.0</Version>
<Detects>
<Detect>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0</keyanme>
</Detect>
</Detects>
</AppInfo>

<Install_Directories>
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

```
<Install_Direcotry>
<OS>Win2000</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win98</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath<keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>WinNT</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
</Install_Directories>

<Files_From_Folders>
<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.* /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%¥*.pdf
</Files_From_Folder>
</Files_From_Folders>
<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat</keyname>
</Registry>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader</keyname>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Persistent Data</keyname>
</Registry>
</Registries>

<Registry_Excludes>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer</keyname>
<value>xRes</value></Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥Adobe¥Viewer</keyname>
<value>yRes</value>
</Registry>

<Registry_Excludes>
```

```
<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_6.0">
<AppInfo>
<Name>Adobe Acrobat Readr 6.0<¥Name>
<Version>6.0</Version>
<Detects>
<Detect>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0</keyname>
</Detect>
</Detects>
<¥AppInfo>

<Install_Directories>
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath </keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win2000</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath </keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win98</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath </keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>WinNT</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath </keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
</Install_Directories>

<Files_From_Folders>
<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥6.0¥*.* /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%¥*.pdf
</Files_From_Folder>
</Files_From_Folders>
<Files_Trough_Registries>
```

```
</Files_Trough_Registries>

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat</keyname>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader</keyname>
</Registry>
</Registries>

<Registry_Excludes>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥AdobeViewer</keyname>
<value>xRes</value>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥Adobe¥Viewer</keyname>
<value>yRes</value>
</Registry>

<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchhProcessing>

<TargetBatchProcessing>
<![CDATA[if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
goto Done:Update50
regfix
"HKCU¥Software¥Adobe¥Acrobat Reader¥5.0"
"HKCU¥Software¥Adobe¥Acrobat Reader¥6.0"
regfix
"HKLM¥Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer"
"HKLM¥Software¥Adobe¥Acrobat Reader¥6.0¥AdobeViewer"
:Done]]>
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_7.0">
<AppInfo>
<Name>Adobe Acrobat Reader 7.0<¥Name>
<Version>6.0</Version>
<Detects>
<Detect>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0</keyname>
</Detect>
</Detects>
<¥AppInfo>

<Install_Directories>
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0¥InstallPath</keyname>
<value>(Default)</value>
```

```
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win2000</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>Win98</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>

<Install_Directory>
<OS>WinNT</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
</Install_Directories>

<Files_From_Folders>
<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥7.0¥*.* /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%¥*.pdf
</Files_From_Folder>
</Files_From_Folders>

<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat</keyname>
</Registry>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader</keyname>
</Registry>
</Registries>

<Registry_Excludes>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0¥AdobeViewer</keyname>
<value>xRes</value>
</Registry>

<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat Reader¥7.0¥Adobe¥Viewer</keyname>
<value>yRes</value>
</Registry>

<Registry_Excludes>
<SourceBatchProcessing>
```

```
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
<![CDATA[
if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
if /i "%SourceApp%" == "Acrobat_Reader_60" goto Update60
goto Done:Update50
regfix
"HKCU¥Software¥Adobe¥Acrobat Reader¥5.0"
"HKCU¥Software¥Adobe¥Acrobat Reader¥7.0"
regfix
"HKLM¥Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer"
"HKLM¥Software¥Adobe¥Acrobat Reader¥7.0¥AdobeViewer"
goto Done:Update60
regfix
"HKCU¥Software¥Adobe¥Acrobat Reader¥6.0"
"HKCU¥Software¥Adobe¥Acrobat Reader¥7.0"
regfix
"HKLM¥Software¥Adobe¥Acrobat Reader¥6.0¥AdobeViewer"
"HKLM¥Software¥Adobe¥Acrobat Reader¥7.0¥AdobeViewer"
:Done]]>
</TargetBatchProcessing>
</Application>
</Applications>
```

第 6 章 インストール

本章では、Rescue and Recovery、Client Security Solution、および指紋認証ユーティリティーをインストールする手順について説明します。System Migration Assistant プログラムのインストール手順は、Lenovo Web サイト http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=MIGR-50889&style=lenovo (英語のサイトです) にある「*System Migration Assistant ユーザーズ・ガイド*」に記載されています。

Rescue and Recovery および Client Security Solution のインストール

Rescue and Recovery および Client Security Solution は、似た方法でインストールされるように設計されていますが、多少の相違点があります。このセクションでは、インストールの類似点およびインストールの相違点について説明します。

Rescue and Recovery および Client Security Solution のインストール・パッケージは、InstallShield 10.5 Premier によって Basic MSI プロジェクトとして開発されました。InstallShield Premier 10.5 は、Windows インストーラーを使用して、アプリケーションをインストールします。これにより、管理者には、コマンド・ラインからのプロパティ値の設定などの、インストールをカスタマイズする多くの機能が提供されます。この章では、Rescue and Recovery セットアップ・パッケージおよび Client Security Solution セットアップ・パッケージの使用および実行方法について説明します。より正しく理解するために、パッケージのインストールを開始するために、章全体をお読みください。

注: これらのパッケージをインストールするときは、以下の Lenovo Web ページに掲載されている README ファイルを参照してください。

http://.lenovo.com/pc/support/site.wss/document.do?lndocid=MIGR-4Q2QAK
(英語のサイトです)

README ファイルには、ソフトウェア・バージョン、サポートされるシステム、システム要件、およびインストール・プロセスに役立つその他の考慮事項に関する最新の情報が含まれています。

インストール要件

このセクションでは、Rescue and Recovery パッケージおよび Client Security Solution パッケージをインストールするためのシステム要件を説明します。最良の結果を得るために、次の Web サイトにアクセスして、ソフトウェアが最新版であることを確認してください。

http://www.ibm.com/jp/pc/think/thinkvantagetech/

IBM から以前に販売された PC でも、指定された要件を満たしていれば、Rescue and Recovery および Client Security Solution がサポートされます。Rescue and Recovery および Client Security Solution がサポートされる IBM PC について詳しくは、http://www.ibm.com/jp/pc/think/thinkvantagetech/ を参照してください。

IBM および Lenovo PC の要件

Rescue and Recovery および Client Security Solution をインストールするには、IBM および Lenovo PC が次の要件を満たしているか、それ以上であることが必要です。

- オペレーティング・システム:Microsoft Windows XP (Service Pack 1 適用済み) または Windows 2000 (Service Pack 3 適用済み) 以上。
- メモリー: 256 MB 以上推奨
  - 共用メモリー設定の場合、共用メモリーの BIOS 設定を 8 MB 以上に設定する必要があります。
  - 非共用メモリー設定の場合、非共用メモリーは 120 MB 以上です。

  注: PC の非共用メモリーが 200 MB 未満である場合でも、Rescue and Recovery は稼働します。ただし、Rescue and Recovery ワークスペースで複数のアプリケーションを起動することができない場合があります。
- Internet Explorer 5.5 以上がインストールされていなければなりません。
- ハードディスク空き容量 2.4 GB。
- 解像度 800 x 600 および 24 ビット・カラーをサポートする VGA 対応ビデオ。
- サポートされるイーサネット・カード。
- ユーザーは管理特権を持っている必要があります。
- ハードウェア・パスワードをリセットする場合の追加要件: NTFS および Windows XP。

Lenovo プリロード・イメージ以外の PC へのインストールのための要件

Lenovo プリロード・イメージ以外の PC へのインストールには、次の要件があります。

インストール要件: ハードディスク空き容量 2.4 GB。基本インストールは 930 MB を使用します。

最小システム・メモリー要件: Rescue and Recovery をインストールするには、128 MB のシステム RAM が必要です。

ハードディスク・ドライブ設定: Rescue and Recovery および Client Security Solution プログラムは、相手先ブランドで販売されるために製造された (OEM) PC (IBM 以外または Lenovo 以外の) の出荷時プリロードではサポートされません。

注: Rescue and Recovery プログラムの場合、OEM PC のハードディスク・ドライブを 129 ページの『デプロイメント・シナリオ 2』の推奨に従って設定する必要があります。

外部メディア (CD/DVD および USB) からの起動のサポート: IBM 以外または Lenovo 以外の PC およびデバイス (USB ハードディスク・ドライブ、CD-R/RW、DVD-R/RW/RAM、または DVD+R/RW) は、以下のうち 1 つ以上の仕様を完全にサポートしている必要があります。

- ATAPI Removable Media Device BIOS Specification
- BIOS Enhanced Disk Drive Services - 2
- Compaq Phoenix Intel® BIOS Boot Specification
- El Torito Bootable CD-ROM Format Specification

- USB Mass Storage Class Specification Overview (各デバイスは、「USB Mass Storage Class Specification Overview」のセクション 2.0 サブクラス・コードのコマンド・ブロック仕様に準拠している必要があります。)
- USB Mass Storage Specification for Bootability

ビデオ要件:

- **ビデオ互換性:** 解像度 800 x 600 および 24 ビット・カラーをサポートする VGA 対応ビデオ
- **ビデオ・メモリー:**
  - 非共用ビデオ・メモリー・システムの場合: 最小 4 MB のビデオ RAM
  - 共用ビデオ・メモリー・システムの場合: 最小 4MB から最大 8 MB をビデオ・メモリーに割り振ることができます。

アプリケーション互換性: フィルター・ドライバーを使用している一部のアプリケーション (アンチウィルス・ソフトウェアなど) は、Rescue and Recovery または Client Security Solution ソフトウェアとの互換性がない場合があります。互換性の問題について詳しくは、次の Web サイトにある Rescue and Recovery または Client Security Solution ソフトウェアに付随する README ファイルを参照してください。

http://www.ibm.com/jp/pc/think/thinkvantagetech/

ユーティリティー: 本書では、いくつかのユーティリティーを使用します。これらのユーティリティーは、次の Web サイトに置かれています。

http://www.ibm.com/jp/pc/think/thinkvantagetech/

Rescue and Recovery のネットワーク・アダプター: Rescue and Recovery ワークスペースは、有線の PCI ベースのイーサネット・ネットワーク・アダプターのみをサポートしています。サポートされる IBM および Lenovo PC の場合、必要なドライバーは Rescue and Recovery ソフトウェアに付属しています。

ご使用の PC の OEM ネットワーク・デバイスがサポートされない場合、PC 固有のネットワーク・ドライバーのサポートを追加する手順について、デバイス・メーカーの資料を参照してください。OEM にドライバーを要求してください。

インストール・コンポーネント

このセクションでは、Rescue and Recovery および Client Security Solution のインストール・コンポーネントについて説明します。

標準的なインストール手順およびコマンド・ライン・パラメーター

Setup.exe は、一連のコマンド・ライン・パラメーターを受け入れます。コマンド・ライン・オプションには、パラメーターを指定することが必要です。この場合、オプションとパラメーターの間にスペースは入れません。例:

```
Setup.exe /s /v"/qn REBOOT="R""
```

は有効ですが、

```
Setup.exe /s /v "/qn REBOOT="R""
```

は無効です。

注: インストールを単独で実行すると (パラメーターを指定せずに setup.exe を実行すると)、デフォルトでは、インストール終了時にユーザーに再起動を促すプロンプトが出されます。プログラムを正しく機能させるには、再起動する必要があります。上記のセクションおよび例のセクションで示すように、サイレント・インストールではコマンド・ライン・パラメーターを使用して再起動を遅らせることができます。

表 13 のパラメーターと説明は、InstallShield Developer のヘルプ文書に記載されています。基本 MSI プロジェクトに適用されないパラメーターは、除かれています。例: [rescue] mailbox = %y%¥antidote, c:¥antidote

表 13.

パラメーター	説明
/a : 管理用インストール	/a スイッチを指定すると、setup.exe で管理用インストールが実行されます。管理用インストールは、データ・ファイルをユーザーが指定したディレクトリーにコピー (および解凍) しますが、ショートカットの作成、COM サーバーの登録、アンインストール・ログの作成は行いません。
/x : アンインストール・モード	/x スイッチを指定すると、setup.exe は以前にインストールした製品をアンインストールします。
/s : サイレント・モード	コマンド setup.exe /s を実行すると、基本 MSI インストール・プログラム用の setup.exe 初期設定ウィンドウは表示されず、応答ファイルは読み取られません。基本 MSI プロジェクトでは、サイレント・インストールの場合、応答ファイルは作成も使用もされません。基本 MSI 製品をサイレントで実行するには、コマンド・ライン setup.exe /s /v/qn を実行します。 (基本 MSI のサイレント・インストールの共通プロパティ値を指定する場合は、 setup.exe /s /v″/qn INSTALLDIR=D:¥Destination″ などのコマンドを使用できます。)
/v : Msiexec への引数の受け渡し	/v 引数を使用して、 msiexe.exe にコマンド・ライン・スイッチと共通プロパティの値を渡します。
/L : 言語のセットアップ	ユーザーは、/L スイッチと 10 進言語 ID を使用して、複数言語インストール・プログラムで使用する言語を指定します。たとえば、ドイツ語を指定するコマンドは setup.exe /L1031 です。 102 ページの表 26 に記載されているすべての言語のインストールがサポートされているわけではありません。

表 13. (続き)

パラメーター	説明
/w : 待機	基本 MSI プロジェクトで引数 /w を指定すると、setup.exe は、インストールが完了するのを待ってから終了します。バッチ・ファイルで /w オプションを使用すると、 setup.exe のコマンド・ライン引数全体を start /WAIT で開始することができます。正しくフォーマットされたコマンドの使用例は、次のとおりです。 `start /WAIT setup.exe /w`

標準 Windows インストーラーの共通プロパティ

Windows インストーラーには、一連の標準組み込み共通プロパティがあります。これらのプロパティをコマンド・ラインで設定して、インストール時の特定の動作を指定することができます。下表に、コマンド・ラインで使用される最も一般的な共通プロパティについて説明します。追加情報については、Microsoft Web サイト http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp (英語のサイトです) を参照してください。

表 14 に、一般に使用される Windows インストーラーのプロパティを示します。

表 14.

プロパティ	説明
TARGETDIR	インストール用の宛先のルート・ディレクトリーを指定します。管理用インストールの場合、このプロパティは、インストール・パッケージのコピー先です。
ARPAUTHORIZEDCDFPREFIX	アプリケーションの更新チャネルの URL。
ARPCOMMENTS	「コントロール パネル」の「プログラムの追加と削除」に「コメント」を提供します。
ARPCONTACT	「コントロール パネル」の「プログラムの追加と削除」に「連絡先」を提供します。
ARPINSTALLLOCATION	アプリケーションの 1 次フォルダーへの完全修飾パス。
ARPNOMODIFY	製品を変更する機能を使用不可にします。
ARPNOREMOVE	製品を削除する機能を使用不可にします。
ARPNOREPAIR	「プログラム」ウィザードの「修復」ボタンを使用不可にします。
ARPPRODUCTICON	インストール・パッケージの基本アイコンを指定します。
ARPREADME	「コントロール パネル」の「プログラムの追加と削除」に README を提供します。
ARPSIZE	アプリケーションの推定サイズ (KB)。
ARPSYSTEMCOMPONENT	「プログラムの追加と削除」のリストにアプリケーションを表示しないようにします。

表 14. (続き)

プロパティ	説明
ARPURLINFOABOUT	アプリケーションのホーム・ページの URL。
ARPURLUPDATEINFO	アプリケーション更新情報の URL。
REBOOT	REBOOT プロパティにより、システムの再起動を促す特定のプロンプトが抑止されます。管理者は通常、一連のインストールを行う際にこのプロパティを使用して、複数の製品を同時にインストールし、最後に一度だけ再起動します。インストール終了時の再起動を使用不可にするには、REBOOT=”R” と設定します。

ログ・ファイルのインストール

ログ・ファイル rrinstall31.txt および cssinstall70.txt は、setup.exe でセットアップが起動すると (メインの install.exe をダブルクリックするか、パラメーターなしでメインの実行可能ファイルを実行するか、msi を解凍して setup.exe を実行します)、%temp% ディレクトリーに作成されます。これらのファイルには、インストール問題のデバッグに使用できるログ・メッセージが含まれています。これらのログ・ファイルは、MSI パッケージからセットアップを直接実行している場合には作成されません。このログ・ファイルには、「プログラムの追加と削除」から実行されるアクションが含まれています。すべての MSI アクションのログ・ファイルを作成するには、レジストリー内のログ・ポリシーを使用可能にすることができます。これを行うには、次の値を作成します。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows¥Installer]
"Logging"="voicewarmup"
```

インストールの例

次の表は、setup.exe を使用したインストールの例です。

表 15.

説明	例
サイレント・インストール (再起動なし)。	`setup.exe /s /v"/qn REBOOT="R""`
管理用インストール。	`setup.exe /a`
管理者用のサイレント・インストール (Rescue and Recovery の解凍先を指定)。	`setup.exe /a /s /v"/qn TARGETDIR="F:¥TVTRR""`
管理用のサイレント・インストール (Client Security Software の解凍先を指定)。	`setup.exe /a /s /v"/qn TARGETDIR="F:¥CSS70""`
サイレント・アンインストール setup.exe /s /x /v/qn。	`setup.exe /s /x /v/qn`
再起動なしのインストールで、Rescue and Recovery の temp フォルダーにインストール・ログを作成。	`setup.exe /v"REBOOT="R" /L*v %temp%¥rrinstall40.log"`
再起動なしのインストールで、Client Security Software の temp フォルダーにインストール・ログを作成。	`setup.exe /v"REBOOT="R" /L*v %temp%¥cssinstall70.log"`

表 15. (続き)

説明	例
ワークスペースをインストールしないインストール setup.exe /vPDA=0。	`setup.exe /vPDA=0`

次の表に、Rescue and Recovery.msi を使用したインストールの例を示します。

表 16.

説明	例
インストール	msiexec /i “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi”
サイレント・インストール (再起動なし)	msiexec /i “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi” /qn REBOOT=”R”
サイレント・アンインストール	msiexec /x “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi” /qn
ワークスペースをインストールしないインストール	msiexec /i “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi” PDA=0

次の表は、Client Security Solution.msi を使用したインストールの例です。

表 17.

説明	例
インストール	`msiexec /i "C:¥CSS70¥Client Security Solution.msi"`
サイレント・インストール (再起動なし)	`msiexec /i "C:¥CSS70¥Client Security Solution.msi" /qn REBOOT="R"`
サイレント・アンインストール	`msiexec /x "C:¥CSS70¥Client Security Solution.msi" /qn`

インストールするソフトウェアのシナリオ

下表に、Rescue and Recovery および Client Security Solution のインストール・シナリオを示します。

表 18.

インストールするソフトウェア	Notes
Client Security Software バージョン 5.4x	Client Security Solution で Rescue and Recovery バージョン 2.0 との共存をサポートしているのは、このバージョンのみです。

表 18. (続き)

インストールするソフトウェア	Notes
Rescue and Recovery バージョン 3.1 のみ	• 製品のフルインストールによってインストールします (Client Security Solution は選択解除)。 • Client Security Solution の一部のコア・コンポーネントは Rescue and Recovery のインストールでもインストールされ、TPM によるバックアップの暗号化と PDA マスター・パスワード構成をサポートします。
Client Security Solution バージョン 7.0	• これは、個別のインストール・パッケージです。 • 製品をフルインストールし、Rescue and Recovery を選択解除して Client Security Solution のみを入れることはできません。 • Client Security Solution コンポーネント (Private Disk と Password Manager) はオプションです。

ソフトウェアの状態変更

ご使用のソフトウェアをアップグレードする際の指針として、次の表を使用してください。この表には、Rescue and Recovery または Client Security Solution の前のバージョンと最新リリースとの互換性について説明されています。

表 19.

インストール済みアプリケーション	Client Security Solution 7.0	OEM 7.0 Client Security Solution	Rescue and Recovery 3.1	OEM Rescue and Recovery 3.1
新規 (既存のアプリケーションなし)	インストール手順に従います。	インストール手順に従います。	インストール手順に従います。	インストール手順に従います。
Client Security Software 5.4x	Client Security Software 5.4x をアンインストールし、Client Security Solution 7.0 をインストールします。注: アンインストールの前に、すべてのデータを暗号化解除してください。	Client Security Software 5.4x をアンインストールし、OEM Client Security Solution をインストールします。注: アンインストールの前に、すべてのデータを暗号化解除してください。	Client Security Software 5.4x をアンインストールし、Rescue and Recovery 3.1 をインストールします。注: アンインストールの前に、すべてのデータを暗号化解除してください。	Client Security Software 5.4x をアンインストールし、OEM Rescue and Recovery 3.1 をインストールします。注: アンインストールの前に、すべてのデータを暗号化解除してください。

表 19. (続き)

インストール済みアプリケーション	Client Security Solution 7.0	OEM 7.0 Client Security Solution	Rescue and Recovery 3.1	OEM Rescue and Recovery 3.1
Client Security Software 5.4x および Rescue and Recovery 2.0	Client Security Software 5.4x をアンインストールし、Rescue and Recovery 3.1 にアップグレードしてから、Client Security Solution 7.0 をインストールします。	インストールしません。	Client Security Software 5.4x をアンインストールし、Rescue and Recovery 3.1 にアップグレードします。	インストールしません。
Client Security Software 5.4x および Rescue and Recovery 3.0	Client Security Software 5.4x をアンインストールし、Rescue and Recovery 3.1 にアップグレードしてから、Client Security Solution 7.0 をインストールします。	インストールしません。	Client Security Software 5.4x をアンインストールし、Rescue and Recovery 3.1 にアップグレードします。	インストールしません。
Client Security Solution 6.0 スタンドアロン	既存のバージョンのアップグレードを促すプロンプトが出されたら、アップグレード指示に従って、セットアップを続行します。	インストールしません。	インストールしません。Client Security Solution 6.0 をアンインストールし、Rescue and Recovery 3.1 をインストールします。Client Security Solution 7.0 にアップグレードします。	インストールしません。Client Security Solution 6.0 をアンインストールし、Rescue and Recovery 3.1 をインストールします。Client Security Solution 7.0 にアップグレードします。
Client Security Solution 6.0 スタンドアロンおよび Rescue and Recovery 3.0 コンボ	Client Security Solution 6.0 をアンインストールします。Rescue and Recovery を 3.1 にアップグレードしてから、Client Security Solution 7.0 をインストールします。	インストールしません。	アップグレード・インストール手順に従います。	インストールしません。
Client Security Solution 7.0	適用されません。	インストールしません。	インストール手順に従います。	インストールしません。
OEM Client Security Solution 7.0	適用されません。	インストールしません。	インストールしません。	インストール手順に従います。
Rescue and Recovery 3.0 コンボのみ、Client Security Solution はなし	Rescue and Recovery を 3.1 にアップグレードしてから、Client Security Solution 7.0 をインストールします。	インストールしません。	アップグレード・インストール手順に従います。	インストールしません。

表 19. (続き)

インストール済みアプリケーション	Client Security Solution 7.0	OEM 7.0 Client Security Solution	Rescue and Recovery 3.1	OEM Rescue and Recovery 3.1
Rescue and Recovery 3.0 OEM	インストールしません。	Rescue and Recovery 3.1 にアップグレードしてから、OEM Client Security Solution 7.0 をインストールします。	インストールしません。	アップグレード・インストール手順に従います。
Rapid Restore® Ultra 3.0 および Rapid Restore	インストール手順に従います。	インストール手順に従います。	インストールしません。Rapid Restore Ultra または Rapid Restore をアンインストールしてから、Rescue and Recovery をインストールしなければなりません。	インストールしません。Rapid Restore Ultra または Rapid Restore をアンインストールしてから、Rescue and Recovery をインストールしなければなりません。
Rescue and Recovery 3.1	インストール手順に従います。	インストールしません。	適用されません。	インストールしません。ご使用のシステムで現行バージョンをアンインストールしてから、Rescue and Recovery 3.1 にアップグレードしなければなりません。
OEM Rescue and Recovery 3.1	インストールしません。	インストール手順に従います。	インストールしません。現行バージョンの Rescue and Recovery をアンインストールし、ThinkPad および ThinkCentre を対象にしたバージョンをインストールします。	適用されません。

注:

1. 以前のバージョンの Rescue and Recovery 1.0、2.0、および 3.0 から取り込まれたバックアップ・ファイルは、Rescue and Recovery バージョン 3.1 でリカバリーすることはできません。
2. ユーザーが Rescue and Recovery 3.1 をサイレント・インストールする場合、Client Security Solution のユーザー・ファイルおよび設定は、インストール時に自動的に削除されます。
3. 製品 (Rescue and Recovery 3.1 または Client Security Solution 7.0) のインストール時に Password Manager と Private Disk を選択するか選択解除するかによって、インストール後のコンポーネントの最終状態が決まります。たとえば、Client Security Solution 7.0 と同時に Password Manager をインストールして、製品のインストール中にその選択を解除した場合、それは、インストールの完了後にはインストールされなくなります。製品 (Rescue and Recovery または Client Security Solution) のサイレント・インストールを実行する場合は、インス

トール・コマンドでそれぞれのプロパティ NOPRVDISK=1 または NOPWMANAGER=1 を設定しない限り、Password Manager も Private Disk もインストールされます。

「プログラムの追加と削除」、またはオリジナル・ソースのユーザー・インターフェースから Client Security Solution 7.0 をアンインストールすると、ユーザーには、Client Security Solution の設定およびデータ・ファイルの削除を促すプロンプトが出されます。コマンド・ラインからサイレント・アンインストールを実行する場合、デフォルトでは Client Security Solution の設定およびデータ・ファイルは削除されますが、アンインストール・コマンドでプロパティ NOCSSCLEANUP=1 を設定すると、このアクションをオーバーライドすることができます。

Rescue and Recovery のインストール

1. Rescue and Recovery のメインの実行可能ファイルは Z180Z1S10010xxUS00.exe です。これは、インストール・ソース・ファイルを解凍し、 Windows インストーラーを使用してインストールを起動する自己解凍型インストール・パッケージです。このファイルには、インストール・ロジックと Windows アプリケーション・ファイルが含まれています。パッケージには、ワークスペース・ファイルは含まれていません。
2. Predesktop Area US Base (約 135 MB): これは、パスワードで保護された ZIP ファイルで、 US ベースのワークスペース全体が含まれています。その名前の形式は、Z180ZAB10xxUS00.tvt です。この場合、*AB* は、ワークスペースの互換性を決定し、*0xx* はワークスペースのレベルです。このファイルは、すべての言語システムにワークスペースをインストールする際に必要です。このファイルは、メイン・インストール・パッケージ (解凍または OEM インストールの場合は、インストール実行可能ファイルまたは Rescue and Recovery.msi のいずれか) と同じディレクトリーになければなりません。この場合の例外は、ワークスペースがすでにインストール済みでアップグレードする必要がない場合、またはインストールを実行する際にコマンド・ラインでプロパティ PDA=0 が設定されており、ワークスペース (あらゆるバージョン) がまだ存在していない場合です。インストール実行可能ファイルには、ファイル pdaversion.txt が含まれています。このファイルには、Windows のそのバージョンと連動可能なワークスペースの最小バージョンが含まれています。インストール実行可能ファイルのインストーラーは、次のロジックを使用してワークスペースを探します。
   - **古い Predesktop Area (Rescue and Recovery 1.0 または 2.X) が存在するか、Predesktop Area が存在しない場合:**

     インストーラーは、最小バージョンの互換コードと等しい互換コード (たとえば、AA、AB) を持ち、レベルが最小バージョン (.tvt ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) 以上の .tvt ファイルを探します。これらの基準を満たすファイルが見つからない場合、インストールは停止します。
   - **新しい (Rescue and Recovery 3.0 以上) Predesktop Area が存在する場合:**

     インストーラーは、現在のワークスペースの互換コードを最小バージョンの互換コードと比較し、その結果に基づいて以下の処理を行います。
     - **現在のコードが最小コードより大きい場合:**

インストーラーは、現在の環境はこのバージョンの Rescue and Recovery と互換性がないというメッセージを表示します。

– **現在のコードと最小コードが同じである場合:**

インストーラーは、現行バージョンのレベルを最小バージョンのレベルと比較します。現行バージョンのレベルが最小バージョンのレベル以上である場合、インストーラーは、最小バージョンの互換コードと等しい互換コード (AA や AB など) を持ち、そのレベルが現行バージョンのレベルより高い .tvt ファイル (.tvt ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) を探します。インストーラーがファイルを見つけられない場合、インストール・プロセスはワークスペースを更新せずに続行されます。現在のレベルが最低レベル未満である場合、インストーラーは、最小バージョンの互換コードと等しい互換コード (AA や AB など) を持ち、レベルが最小バージョンのレベル以上の .tvt ファイル (.tvt ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) を探します。これらの基準を満たすファイルが見つからない場合、インストールは停止します。

– **現在のコードが最小コードより小さい場合:**

インストーラーは、最小バージョンの互換コードと等しい互換コード (たとえば、AA、AB) を持ち、レベルが最小バージョン (.tvt ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) 以上の .tvt ファイルを探します。これらの基準を満たすファイルが見つからない場合、インストールは停止します。

• Predesktop Area の言語パック (それぞれ約 5 から 30 MB): Rescue and Recovery 3.1 でサポートされる Rescue and Recovery ワークスペースの場合は、16 の言語パックがあります。各言語パックは、Z180ZAB10xxCC00.tvt 形式で命名されており、この場合、CC は言語を表します。英語以外のシステム、またはサポートされない言語のシステムにワークスペースをインストールする場合は、これらのファイルのいずれかが必要です。また、そのファイルは、メイン・インストールおよび US ワークスペースの .tvt ファイルと同じディレクトリーに置く必要があります。ワークスペースをインストールまたは更新する際に言語パックが必要になると、インストールは、インストール実行可能ファイルに含まれているバージョン・ファイルに必要な最小レベルの言語パックを探します。インストールは、すでにインストールされている現在の言語パックより大きい言語パックの .tvt ファイル、および必要な最小バージョン以上の言語パックの .tvt ファイルも探します。

以下のリストは、Rescue and Recovery バージョン 3.1 でサポートされている言語です。

– ブラジル・ポルトガル語
– ポルトガル語
– デンマーク語
– オランダ語
– 英語
– フィンランド語

– フランス語
– ドイツ語
– イタリア語
– 日本語
– 韓国語
– ノルウェー語
– スペイン語
– スウェーデン語
– 中国語 (簡体字)
– 中国語 (繁体字)

Rescue and Recovery のカスタム共通プロパティ

Rescue and Recovery プログラムのインストール・パッケージには、一連のカスタム共通プロパティが含まれています。インストールを実行する際は、これらのプロパティをコマンド・ラインで設定することができます。使用可能なカスタム共通プロパティは、以下のとおりです。

表 20.

プロパティ	説明
PDA	ワークスペースをインストールするかどうかを指定します。デフォルト値は 1 です。1 = ワークスペースをインストールします。0 = ワークスペースをインストールしません。注: この設定は、いずれかのバージョンのワークスペースがすでに存在している場合は使用されません。
CIMPROVIDER	Common Information Model (CIM) プロバイダー・コンポーネントをインストールするかどうかを指定します。デフォルトはこのコンポーネントをインストールしません。このコンポーネントをインストールする場合は、コマンド・ラインで CIMPROIVIDER=1 を指定します。
EMULATIONMODE	TPM が存在する場合でも、強制的にエミュレーション・モードでインストールを実行するように指定します。エミュレーション・モードでインストールするには、コマンド・ラインで EMULATIONMODE=1 と設定します。
HALTIFTPMDISABLED	TPM が使用不可状態で、インストールがサイレント・モードで実行されている場合、デフォルトではインストールをエミュレーション・モードで進めます。インストールをサイレント・モードで実行するときは、HALTIFTPMDISABLED=1 プロパティを使用して、 TPM が使用不可の場合にインストールを停止します。

表 20. (続き)

プロパティ	説明
ENABLETPM	インストールで TPM を使用可能にできないようにするには、コマンド・ラインで ENABLETPM=0 を設定します。
NOCSSWIZARD	管理者がログオンし、まだ登録していないときに Client Security Solution ウィザードが表示されないようにするには、コマンド・ラインで NOCSSWIZARD=1 を設定します。このプロパティは、Client Security Solution はインストールしても、システムの構成は後でスクリプトを使用して行う場合に適しています。
CSS_CONFIG_SCRIPT	ユーザーがインストールを完了し、再起動した後に構成ファイルを実行するには、CSS_CONFIG_SCRIPT=”*filename*” または “*filename password*” を設定します。
SUPERVISORPW	コマンド・ラインで SUPERVISORPW=”*password*” と設定すると、スーパーバイザー・パスワードが提供され、サイレント・インストール・モードでも非サイレント・インストール・モードでも、チップが使用可能になります。チップが使用不可で、インストールをサイレント・モードで実行する場合、チップを使用可能にするには正しいスーパーバイザー・パスワードを入力する必要があります。パスワードが正しくないと、チップは使用可能になりません。

Rescue and Recovery のディスク・イメージへの組み込み

他社製複製ツールを使用して、Rescue and Recovery が組み込まれたディスク・イメージを作成することができます。本デプロイメント・ガイドでは、PowerQuest および Ghost について基本的な情報を記載しています。

注: イメージを作成する場合、マスター・ブート・レコードを取り込む必要があります。マスター・ブート・レコードは、Rescue and Recovery ワークスペースが正常に機能する上で重要です。

PowerQuest Drive Image ベースのツールと Rescue and Recovery の併用

PowerQuest DeployCenter ツール PQIMGCTR が X:¥PQ にインストールされている場合、次のスクリプトにより Rescue and Recovery がインストールされたイメージの作成とデプロイメントを行うことができます。

最小スクリプト・ファイル:

表 21. X:¥PQ¥RRUSAVE.TXT

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する。
`SELECT PARTITION ALL` (タイプ 12 区画またはイメージ内に複数の区画がある場合に必要。)	すべての区画を選択する。
Store with compression high	イメージを保管する。

表 22. X:¥PQ¥RRDEPLY.TXT

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する。
`DELETE ALL`	すべての区画を削除する。
`SELECT FREESPACE FIRST`	最初の空き領域を選択する。
`SELECT IMAGE ALL`	イメージのすべての区画を選択する。
`RESTORE`	イメージを復元する。

イメージ作成:

表 23. X:¥PQ¥PQIMGCTR / CMD=X:¥PQ¥RRUSAVE.TXT /MBI=1 / IMG=X:¥IMAGE.PQI

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する。
`X:¥PQ¥PQIMGCTR`	イメージ・プログラムを作成する。
`/CMD=X:¥PQ¥RRUSAVE.TXT`	PowerQuest スクリプト・ファイル。
`/MBI=1`	Rescue and Recovery ブート・マネージャーを取り込む。
`/IMG=X:¥IMAGE.PQI`	イメージ・ファイルを作成する。

イメージ・デプロイメント:

表 24. X:¥PQ¥PQIMGCTR / CMD=X:¥PQ¥RRDEPLY.TXT /MBI=1 / IMG=X:¥IMAGE.PQI

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する。
`X:¥PQ¥PQIMGCTR`	イメージ・プログラムを作成する。
`/CMD=X:¥PQ¥RRDEPLY.TXT`	PowerQuest スクリプト・ファイルを作成する。
`/MBR=1`	Rescue and Recovery ブート・マネージャーを復元する。
`/IMG=X:¥IMAGE.PQI`	イメージ・ファイルを作成する。

Symantec Ghost ベースのツールと Rescue and Recovery の併用

Ghost イメージを作成する場合、コマンド・ライン・スイッチ `-ib` を使用して Rescue and Recovery ブート・マネージャーを取り込む必要があります。また、イメージにはディスク全体およびすべての区画を取り込む必要があります。 Ghost について詳しくは、Symantec が提供している資料を参照してください。

Rescue and Recovery の環境変数

次の表に、Rescue and Recovery のインストール時に作成される環境変数を示します。これらの変数は、コマンド・プロンプトからスクリプトを作成する場合または該当するディレクトリーに変更する場合に使用できます。たとえば、コマンド・プロンプトから Rescue and Recovery フォルダーに変更する場合、“CD %rr%” と入力して Enter を押します。

表 25.

環境変数	ディレクトリー
%rr%	c:¥Program Files¥Lenovo¥Rescue and Recovery
%SWSHARE%	c:¥Program Files¥Lenovo
%TVTCOMMON%	c:¥Program Files¥Common Files¥Lenovo

注: 変数の完全なリストを見るには、Rescue and Recovery がインストールされている PC で ’set’ コマンドを実行します。

Client Security Solution のインストール

Client Security Solution 7.0 のインストールは、単一の実行可能ファイル (約 55 MB) で構成されています。これは、インストール・プロジェクト・ソースから作成された setup.exe です。setup.exe ファイルは、ビルド・プロセスで、プロジェクト ID、メディア・タイプ、ビルド・レベル、国別コード (この場合は常に US)、およびパッチ・コードを表す名前 (たとえば Z256Z1001US00.exe) に変更されます。これは、インストール・ソース・ファイルを解凍し、 Windows インストーラーを使用してインストールを起動する自己解凍型インストール・パッケージです。このファイルには、インストール・ロジックと Windows アプリケーション・ファイルが含まれています。

次の表に、Client Security Solution の言語パックを示します。

表 26.

言語	ID
中国語 (簡体字)	2052
中国語 (繁体字)	1028
デンマーク語	1030
オランダ語 (標準)	1043
英語	1033
フィンランド語	1035
フランス語	1036
ドイツ語	1031
イタリア語	1040

表 26. (続き)

言語	ID
日本語	1041
韓国語	1042
ノルウェー語 (ブークモール)	1044
ポルトガル語 (ブラジル)	1046
ポルトガル語 (標準)	2070
スペイン語	1034
スウェーデン語	1053

Client Security Software カスタム共通プロパティ

Client Security Software プログラムのインストール・パッケージには、インストールの実行時にコマンド・ラインで設定できる、一連のカスタム共通プロパティが含まれています。使用可能なカスタム共通プロパティは、以下のとおりです。

表 27.

プロパティ	説明
EMULATIONMODE	TPM が存在する場合でも、強制的にエミュレーション・モードでインストールを実行するように指定します。エミュレーション・モードでインストールするには、コマンド・ラインで EMULATIONMODE=1 と設定します。
HALTIFTPMDISABLED	TPM が使用不可状態で、インストールがサイレント・モードで実行されている場合、デフォルトではインストールをエミュレーション・モードで進めます。インストールをサイレント・モードで実行するときは、HALTIFTPMDISABLED=1 プロパティを使用して、 TPM が使用不可の場合にインストールを停止します。
ENABLETPM	インストールで TPM を使用可能にできないようにするには、コマンド・ラインで ENABLETPM=0 を設定します。
NOPRVDISK	SafeGuard PrivateDisk の機能がインストールされないようにするには、コマンド・ラインで NOPRVDISK=1 を設定します。サイレント・インストールで使用してください。ただし、ユーザー・インターフェース・インストールでも使用できます。ユーザー・インターフェース・インストールでは、SafeGuard PrivateDisk 機能はカスタム・セットアップ画面には表示されません。

表 27. (続き)

プロパティ	説明
NOPWMANAGER	Password Manager の機能がインストールされないようにするには、コマンド・ラインで NOPWMANAGER=1 を設定します。サイレント・インストールで使用してください。ただし、ユーザー・インターフェース・インストールでも使用できます。ユーザー・インターフェース・インストールでは、Password Manager 機能はカスタム・セットアップ画面には表示されません。
NOCSSWIZARD	管理者がログオンし、まだ登録していないときに Client Security Solution ウィザードが表示されないようにするには、コマンド・ラインで NOCSSWIZARD=1 を設定します。このプロパティは、Client Security Solution はインストールしても、システムの構成は後でスクリプトを使用して行う場合に適しています。
CSS_CONFIG_SCRIPT	ユーザーがインストールを完了し、再起動した後に構成ファイルを実行するには、CSS_CONFIG_SCRIPT="*filename*" または "*filename password*" を設定します。
SUPERVISORPW	コマンド・ラインで SUPERVISORPW="*password*" と設定すると、スーパーバイザー・パスワードが提供され、サイレント・インストール・モードでも非サイレント・インストール・モードでも、チップが使用可能になります。チップが使用不可で、インストールをサイレント・モードで実行する場合、チップを使用可能にするには正しいスーパーバイザー・パスワードを入力する必要があります。パスワードが正しくないと、チップは使用可能になりません。

指紋認証ユーティリティーのインストール

指紋認証ユーティリティー・プログラムの setup.exe ファイルは、開始時に以下のパラメーターを指定できます。

サイレント・インストール

指紋認証ユーティリティーのサイレント・インストールを実行できます。CD-ROM ドライブの Install フォルダーで、 setup.exe を実行してください。

このときの構文は次のようになります。

```
Setup.exe PROPERTY=VALUE /q /i
```

ここで、*q* はサイレント・インストール、*i* はインストールを表します。例:

```
Setup.exe INSTALLDIR="F:¥Program Files¥ThinkVantage fingerprint software" /q /i
```

このソフトウェアをアンインストールするには、/i の代わりに /x パラメーターを使用します。

```
Setup.exe INSTALLDIR="F:¥Program Files¥ThinkVantage fingerprint software" /q /x
```

System Management Server (SMS) のインストール

System Management Server (SMS) のインストールもサポートされています。SMS 管理者コンソールを開きます。新規パッケージを作成して標準的なパッケージ・プロパティを設定します。そのパッケージを開き、「プログラム」項目で「新規プログラム」を選択します。コマンド・ラインに次のように入力します。

Setup.exe /m *yourmiffilename* /q /i

サイレント・インストールの場合と同じパラメーターが使用できます。

Setup では、通常はインストール・プロセス終了時に再起動します。インストール中は再起動せず、後で (さらにいくつかのプログラムをインストールしてから) 再起動する場合は、プロパティ・リストに REBOOT=″ReallySuppress″ を追加します。

オプション

指紋認証ユーティリティーでは以下のオプションがサポートされています。

表 28.

パラメーター	**説明**
CTRLONCE	コントロール・センターを一度だけ表示します。デフォルトは 0 です。
CTLCNTR	始動時にコントロール・センターを実行します。デフォルトは、1 です。
DEFFUS	• 0 = Fast User Switching (FUS) 設定を使用しません。 • 1 = FUS 設定の使用を試みます。 デフォルトは 0 です。
INSTALLDIR	指紋認証ユーティリティーのデフォルトのインストール・ディレクトリーに入ります。
OEM	• 0 = サーバー・パスポートまたはサーバー認証のインストールをサポート • 1 = スタンドアロン PC モードのみ (ローカル・パスポート)
PASSPORT	インストール時に設定されるデフォルトのパスポート・タイプになります • 1 = デフォルト - ローカル・パスポート • 2 = サーバー・パスポート デフォルトは、1 です。

表 28. (続き)

パラメーター	説明
SECURITY	• 1 = セキュア・モードのインストールをサポート • 0 = インストールしない。便利モードのみ存在
SHORTCUTFOLDER	「スタート」メニューのショートカット・フォルダーのデフォルト名になります。
REBOOT	Really Suppress に設定すると、インストール中は、プロンプトを含むすべての再起動を行わないようにします。
DEVICEBIO	ユーザーにより使用されるデバイス・タイプを構成します。登録タイプ: • DEVICEBIO=#3 - デバイス・セクターは最初に登録する前に使用されます。 • DEVICEBIO=#0 - ハードディスクへの登録が使用されます • DEVICEBIO=#1 - CompanionChip への登録が使用されます

第 7 章 Antidote Delivery Manager のインフラストラクチャー

Antidote Delivery Manager は、管理者からの命令を各システムに配信し、ウィルスまたはワームに対抗するためのコマンドをサポートすることによって働きます。管理者は、各システムで望ましいアクションを含むスクリプトを用意します。リポジトリー機能は、スクリプトを数分間以内に PC に安全に配信し、コマンドを実行します。コマンドには、ネットワーク接続の制限、ユーザーへのメッセージ表示、バックアップからファイル復元、ファイルのダウンロード、他のシステム・コマンドの実行、PC を再起動して同じオペレーティング・システムに入ったり、 Rescue and Recovery ワークスペースに入ったりと切り替えたりすることが含まれます。リポジトリー機能とコマンドは両方とも、通常のオペレーティング・システム (Windows XP など) または Rescue and Recovery ワークスペースで働きます。

ウィルスに対抗する総合的な戦略は、悪意のあるコードの広がりと損害を低減し、パッチを当てて各 PC をクリーンアップしてから、復元された PC をネットワークに戻すことです。非常に破壊的で素早く広がるウィルスの場合、PC をネットワークから削除し、Rescue and Recovery ワークスペースですべての修復操作を行う必要があります。これが一番安全な方法ですが、通常の作業時間内にこの方法が取られる場合には、ユーザーの作業を中断させることになります。場合によっては、Rescue and Recovery ワークスペースへの移行のタイミングを遅らせたり、ネットワーク機能を制限することによって移行を回避したりできます。次のステップは、パッチやクリーンアップ用のコードをダウンロードし、クリーンアップ・コードを実行して、パッチのインストールの準備をすることです。一般に、パッチはオペレーティング・システムの稼働中にインストールされるようになっていますが、クリーンアップおよびその他の操作は Rescue and Recovery ワークスペースで行う方が適切です。修正処置が完了すると、PC は、Windows XP が動作し、ネットワーク設定が復元された状態で、通常の操作に復元することができます。

次の 2 つのセクションでは、リポジトリー操作およびコマンドについて詳細に説明します。次に、機能のインストールおよび設定が紹介されます。以下のセクションは、テスト、破壊的なウィルスへの対応、ワイヤレスまたは仮想プライベート・ネットワーク (VPN) によって接続された PC へのアドレッシング、および破壊度が軽い問題の修正のために PC をどのように使用するかといった一般的な作業の例を示します。

リポジトリー

リポジトリー機能は、各 PC で稼働し、管理者からの新しいメッセージがないか定期的に確認します。確認は、スケジュールされた時間間隔で、またはいくつかの注目するイベント (たとえば、起動、中断または休止からの再開、新しいネットワーク・アダプターの検出、および新しい IP アドレスの割り当て) が発生したときに行われます。リポジトリー機能は、登録されたディレクトリー (Windows 共有ロケーション、 HTTP の URL、FTP の URL) にメッセージがないかを探します。複数のメッセージが見付かる場合は、それらを名前をソートした順で処理します。一度に 1 つのメッセージのみが処理されます。メッセージは一度のみ正常に処理されま

す。メッセージの処理が失敗すると、デフォルトでは、再び試行されることはありませんが、失敗時に再試行することを、メッセージ内に指定できます。

メッセージをリポジトリー機能によって処理されるフォルダー内に配置する前に、管理者がメッセージをパッケージしておく必要があります。パッケージを作成する場合、管理者はメッセージを構成するすべてのファイルをフォルダー (またはそのサブフォルダー) に配置します。ファイルのうち 1 つは、基本コマンド・スクリプトである "go.rrs" という名前が付いている必要があります。管理者は、オプションでこのメッセージに署名キーを使用できますが、使用する場合、キーはすべてのターゲット・システムに使用可能である必要があります。リポジトリー機能は、パッケージの保全性をチェックし、署名が提供されているかどうかチェックし、go.rrs を実行する前にすべてのファイルをローカル・フォルダーに展開します。

基本コマンド・スクリプト・ファイル (go.rrs) は、Windows コマンド・ファイルの構文に従います。これには、正しい Windows コマンドおよび、次のセクションでリストするコマンドを含むことができます。また、Python コマンド・インタープリターが Rescue and Recovery ワークスペースの一部としてインストールされるので、Python スクリプトも go.rrs スクリプトから呼び出すことができます。

スクリプトの実行の最後に、メッセージから展開されたファイルはすべて削除されるので、スクリプトの終了後にファイルが必要な場合 (たとえば、再起動時のパッチのインストール) には、ファイルをメッセージ・フォルダーから移動する必要があります。

各 PC は、メッセージを確認するリポジトリーに関する設定を持っています。IT 管理者が、多数の PC をグループに分割して、各グループに異なるリポジトリー (ネットワーク共有) を割り当てることが適切な場合があります。たとえば、PC はファイル・サーバーへの接近性によって地理的にグループ化することができるでしょう。あるいは、PC は組織別 (技術、営業、またはサポートなど) にグループ化することもできます。

Antidote Delivery Manager および Windows コマンド

Antidote Delivery Manager システムは、PC の操作を容易にするためのいくつかのコマンドを提供します。メッセージを作成したり、設定値を調整したりするためのコマンドに加えて、ネットワークの制御、オペレーティング・システムの状態の決定および制御、システム・インベントリーからの XML ファイルの検査、ユーザーへのクライアント PC 上の Antidote Delivery Manager スクリプトの進行状況を通知するといったコマンドがあります。NETWK コマンドは、ネットワークを有効または無効にしたり、ネットワークを限定されたネットワーク・アドレスのグループ内に制限したりします。INRR コマンドは、Windows XP オペレーティング・システムが稼働中であるかどうか、あるいは PC が Rescue and Recovery ワークスペースにあるかどうかを判別するために使用できます。REBOOT コマンドは、PC をシャットダウンして、Windows XP または Rescue and Recovery を起動するよう指定するために使用できます。MSGBOX アプリケーションでは、ポップアップ・ボックスでメッセージを表示してユーザーに通知を行うことができます。メッセージ・ボックスはオプションで「OK」および「取消」ボタンを含むことができるので、メッセージはユーザーからの入力に基づいて異なる動作を行うことができます。

一部の Microsoft コマンドは Antidote Delivery Manager にも使用できます。許可されるコマンドには、コマンド・シェルに内蔵のコマンドすべて (たとえば、DIR や CD) が含まれます。その他の有用なコマンド、たとえばレジストリーを変更するための reg.exe やディスクの整合性を検査するための chkdsk.exe が使用可能です。

Antidote Delivery Manager の使用方法

Antidote Delivery Manager システムを使用して、多種多様なタスクを実行することができます。以下の例は、このシステムをどのように使用できるかを示しています。

- **単純なシステムのテスト - 通知の表示**

  このシステムの最も基本的な使用法は、ユーザーへ文章を 1 つ表示することです。このテストを実行したり、他のスクリプトをデプロイメントの前にテストするための最も簡単な方法は、このメッセージを、管理者の PC のローカル・フォルダーであるリポジトリーに配置することです。このように配置することで、他の PC に影響を与えずに、スクリプトを素早くテストできます。
- **スクリプトの準備およびパッケージ化**

  go.rrs スクリプトを Antidote Delivery Manager をインストール済みのいずれかの PC に書き込みます。`MSGBOX /MSG "Hello World" /OK` という行を含むようにします。go.rrs を含むフォルダーで APKGMSG コマンドを実行して、メッセージを作成します。
- **スクリプトの実行**

  メッセージ・ファイルを PC のリポジトリー・フォルダーのいずれか 1 つに配置し、正しく動作するか監視します。メール・エージェントが次回実行されると、メッセージ・ボックスは「皆さんこんにちは (Hello World)」テキストを表示します。このようなスクリプトは、ネットワーク・リポジトリーをテストしたり、中断モードから再開したときのリポジトリーのチェックなどの機能を明示したりするためにもよい方法です。

大規模なワームの攻撃

この例では、ウィルスに対抗するための考えられる 1 つのアプローチを明示します。基本的なアプローチは、ネットワークをオフにしてから、再起動して Rescue and Recovery に入り、修正ファイルを取得し、修復作業を実行してから、起動して Windows XP に戻り、パッチをインストールし、最後にネットワークを元に戻すことです。これらすべての機能は、フラグ・ファイルと RETRYONERROR コマンドを使用して、1 つのメッセージを用いて実行することができます。

1. **ロックダウン・フェーズ**

   ロックダウン・フェーズを実行するには、ユーザーにこれから何が起こるか通知します。攻撃がそれほど重大でない場合には、管理者はユーザーに修正を先に延ばすという選択肢を与えることができます。最も保守的なケースでは、このフェーズは、ネットワークを無効にし、エンド・ユーザーが処理中の作業を保存するよう 15 分間などの短い時間を与えるために使用することもできます。RETRYONERROR コマンドを使用して、スクリプトを実行中にしたまま、PC を再起動して Rescue and Recovery ワークスペースに入ることができます。

2. **コード配信フェーズおよび修復フェーズ**

   ネットワークを無効にし、再起動して Rescue and Recovery ワークスペースに入ることにより感染の恐れは取り除かれたので、追加のコードを取得して、修復作業を行うことができます。ネットワークを有効にするか、追加のファイルを取得するために特定のアドレスのみが必要な時間の間許可されるようにできます。Rescue and Recovery ワークスペースに入っている間に、ウィルス・ファイルを削除したり、レジストリーをクリーンアップすることができます。残念ながら、パッチは Windows XP が稼働中であると想定しているため、新しいソフトウェアまたはパッチをインストールすることはできません。ネットワークが無効のまま、ウィルス・コードがすべて削除された状態で、再起動して Windows XP に入り、修復を完了するのが安全です。このときに書き込まれたタグ・ファイルは、再起動後にスクリプトをパッチ・セクションに誘導します。

3. **パッチおよびリカバリー・フェーズ**

   PC が再起動して Windows XP に入るとき、Antidote Delivery Manager は、ユーザーがログインする前に処理を再開します。パッチはこの時点でインストールする必要があります。新しくインストールしたパッチが PC を再起動するよう要求する場合は、PC を再起動させることができます。すべてのクリーンアップとパッチが完了したら、ネットワークを有効にすることができ、ユーザーは、通常の操作が可能であるという通知を受けます。

小規模なアプリケーション更新

すべての管理業務が、先に説明したような徹底した対策を要求するわけではありません。パッチが入手可能であるが、ウィルスから攻撃を受けていない場合には、より緩やかなアプローチが適切なことがあります。

単一のスクリプトで、RETRYONERROR コマンドおよびタグ・ファイルを使用して、操作を制御することができます。

1. **ダウンロード・フェーズ**

   このプロセスは、ユーザーにパッチがダウンロードされるが、後でインストールすればよいことを通知するメッセージ・ボックスで始まります。その次に、パッチをサーバーからコピーすることができます。

2. **パッチ・フェーズ**

   パッチ・コードをインストールする準備ができたので、ユーザーに警告して、インストールを開始するときが来ました。ユーザーが遅延を要求する場合は、遅延を追跡するためにタグ・ファイルを使用することもできます。おそらく後でパッチをインストールする要求は、より緊急性の高いものになるでしょう。Antidote Delivery Manager は、ユーザーが電源をオフにするか、PC を再起動する場合でもこの状態を保持します。ユーザーがすべての処理を完了し、システムを再起動する準備ができたら、パッチがインストールされ、必要であれば、PC は再起動します。

重要: システムを復元して再起動した後、再びシステムを再起動して、変更内容を有効にします。

VPN およびワイヤレス・セキュリティーの対応

Rescue and Recovery ワークスペースは、現在、リモート・アクセス Virtual Private Networks (VPN) やワイヤレス・ネットワーク接続をサポートしていません。 PC が Windows XP でこれらのネットワーク接続のいずれかを使用しており、その後再起動して Rescue and Recovery に入る場合、ネットワークへの接続は失われます。したがって、Rescue and Recovery ではファイルおよび修正をダウンロードするためにネットワークが使用できないので、先の例にあったようなスクリプトは動作しません。

解決策は、必要なファイルをすべて元のメッセージにパッケージしておくか、再起動する前に必要なファイルをダウンロードすることです。すべての必要なファイルを、go.rrs のあるフォルダーに配置します。スクリプト・ファイルは、必要なファイルをスクリプトが終了する (クライアント・システムで go.rrs を含むディレクトリーが削除される) 前に、最終的な位置に移動する必要があります。パッチをメッセージ・ファイルの中に入れるのは、パッチが非常に大きい場合には、実用的でありません。この場合は、ユーザーに、ネットワークがパッチを含むサーバー以外に対して制限されることを通知する必要があります。そうすれば、パッチは、まだ Windows XP にいる間にダウンロードできます。これにより、Windows XP がウィルスにさらされる時間が延びるとはいえ、余分にかかる時間はおそらくそれほど長くありません。

Virtualization Module for Antidote Delivery Manager

Virtualization Module for Antidote Delivery Manager は、貴重なデータや PC を有害なウィルスやワームから保護するのに役立ちます。Virtualization Module for Antidote Delivery Manager は、PC の安全性と管理の容易性が向上するよう設計されています。

管理者は Virtualization Module for Antidote Delivery Manager を使用して、脅威が確認された場合にリモート側でネットワークから端末を切断できます。管理者は、感染した端末をリモートからシャットダウンすることもできます。すべての脅威が存在していない場合は、Rescue and Recovery ワークスペースでシステムを再起動して、壊れている可能性のあるファイルをすべて回復できます。

要件

以下の要件は、Virtualization Module for Antidote Delivery Manager を操作する上で重要です。

- Internet Explorer 6.0 以上。
- PC に Windows XP Professional または Home Edition、Service Pack 2。
- サーバーに Windows CE。
- Antidote Delivery Manager がインストール済み。
- Rescue and Recovery 3.1 がインストール済み。
- 512 MB のメモリー。
- 30 MB のディスク空き容量。
- NTFS 区画へのインストール。

- バーチャライゼーション・テクノロジーと互換性のあるインテル® プロセッサー (一部の Lenovo PC でのみ使用可能)。
- BIOS で使用可能なインテル バーチャライゼーション・テクノロジー・プロセッサー。
- 管理者特権を使用するログオン。

注: サーバーと PC の間の通信は認識されないように設計されています。管理者は Web ブラウザーを備えた PC と対話します。サーバーでは、Virtualization Module for Antidote Delivery Manager は開かれません。

インストール

Virtualization Module for Antidote Delivery Manager プログラムをインストールする前に、バーチャライゼーション・テクノロジー・プロセッサーが有効になっていることを確認します。バーチャライゼーション・テクノロジー・プロセッサーを有効にするには、次のステップを実行します。

1. PC の電源がオフになっている状態で、PC の電源を入れます。
2. F1 キーを押し、ロゴが表示されるか、ビープ音が聞こえてから放します。
3. プロンプトが出されたら、現在のパスワードを入力します。
4. 通常は拡張画面に表示されるインテル バーチャライゼーション・テクノロジー行項目にナビゲートします。
5. インテル バーチャライゼーション・テクノロジー行項目を有効にします。
6. F10 を押して、セットアップ・ユーティリティーを保管して終了します。
7. Enter を押します。

Virtualization Module for Antidote Delivery Manager プログラムをインストールするには、次のステップを実行します。

1. PC を起動します。
2. 開いているプログラムをすべて閉じます。
3. Virtualization Module for Antidote Delivery Manager インストール CD を挿入します。

   注: インストール CD が自動的に開始しない場合は、次のステップを実行します。

   a. Windows デスクトップから、「スタート」をクリックしてから、「ファイル名を指定して実行」をクリックします。
   b. d:¥setup.exe と入力します (ここで、*d* は Rescue and Recovery インストール CD が入っている CD または DVD ドライブのドライブ名です)。
   c. 画面に表示される指示に従います。

   CD が損傷しているか、読み取り不能である場合、購入先にお問い合わせください。

注: Virtualization Module for Antidote Delivery Manager のインストールを正常に完了するには、BIOS でインテル バーチャライゼーション・テクノロジー・オプショ

ンを有効にする必要があります。デフォルトで、このプログラムは有効になっています。有効になっていない場合は、BIOS に入ってこのオプションを有効にしてください。

概要

このセクションでは、Virtualization Module for Antidote Delivery Manager プログラムの概要について説明します。

下表に、ネットワーク状況およびネットワーク接続に関する情報を示します。

表 29. ネットワークの状況および接続

モジュール	説明
ネットワーク状況	2 種類のセクション内に情報が表示されます。その 1 つは Windows IP 構成で、「ホスト名」、「WINs プロキシー」、「ノード・タイプ)、「DNS サフィックス」、「IP ルーティング」、および「検索リスト」などがあります。
ネットワーク状況	「接続固有の DNS サフィックス」、「IP アドレス」、「説明」、「サブネット・マスク」、「物理アドレス」、「デフォルト・ゲートウェイ」、「DHCP」、「自動構成」などの情報が表示されます。
ネットワークを無効にする	リモート側でネットワークから端末を切断できます。
ネットワークを有効にする	接続を再び有効にすることができます。
ネットワーク修復	ネットワーク接続を修復できます。

下表に、システム状況および管理に関する情報を示します。

表 30. システムおよび管理

モジュール	説明
システム	壊れたファイルのリカバリーに役立ちます。
管理	サーバー・アクセスやユーザー・アカウントを管理できます。メニュー・オプション「サーバー」および「ユーザー・アカウント」が表示されます。
Windows XP ネットワークの停止	ネットワーク接続を停止できます。
再起動	ウィルスやワームの脅威があった端末をリモートから再起動できます。

下表に、システムの正常性およびヘルプに関する情報を示します。

表 31. システムの正常性およびヘルプ

モジュール	説明
状況	システムの正常性をモニターし、正常性に関する状況を表示できます。
ログ	ログ・ファイルを表示できます。

証明書のインストール

Virtualization Module for Antidote Delivery Manager プログラムのユーザー・インターフェースは、Web ベースで、通信に CA (認証局) ルート証明書を使用します。デフォルトの証明書はインストールされています。このデフォルトの証明書を使用するか、デフォルトの証明書をカスタマイズするか、独自のカスタム証明書を使用することができます。 Virtualization Module for Antidote Delivery Manager プログラムと通信するには、これらの証明書をインストールする必要があります。次のステップで、証明書のインストール方法について説明します。

1. Windows Internet Explorer などの Web ブラウザーを開きます。
2. アドレス・フィールドに次の IP アドレスを入力します。192.168.0.12
3. Internet Explorer の「セキュリティの警告」で、「**証明書の表示**」をクリックします。
4. 「全般」タブで「**証明書のインストール**」をクリックするか、既存の証明書を使用する場合は「詳細設定」タブの「値」フィールドにあるシリアル番号を書き留めます。
5. 認証プロンプトの「ユーザー ID」および「パスワード」フィールドにユーザー ID とパスワードを入力します。

   注: ユーザー ID およびパスワードが認証されない場合、続けてユーザー ID とパスワードの入力を求めるプロンプトが出されます。認証プロンプトで要求されるユーザー ID とパスワードは、サーバー PC でセットアップされる必要があります。このユーザー ID およびパスワードは、Windows の「コントロール パネル」にある「ユーザー アカウント」でセットアップします。 Virtualization Module for Antidote Delivery Manager では、この「ユーザー アカウント」で設定されたパスワードが必要です。
6. Virtualization Module for Antidote Delivery Manager プログラムのメインメニューから、「**管理および構成**」をクリックします。
7. 「アップロード (Upload)」フィールドで「**参照**」をクリックし、証明書を参照します。証明書のファイル拡張子は .pfx になります。
8. パスワードを入力します。
9. 「**実行依頼**」をクリックします。ファイルが正常にアップロードされたことを通知するプロンプトが表示されます。
10. Virtualization Module for Antidote Delivery Manager メニューから「**ターゲット PC の再起動**」をクリックします。これにより、サーバー PC が再起動し、インストールされた証明書が有効になります。

コマンド

以下のコマンドは、Virtualization Module for Antidote Delivery Manager プログラムの制御に使用されます。

- /E - すべてのネットワークを有効にする (/ip および /nm は無視されます)。
- /D - すべてのネットワークを無効にする (/ip および /nm は無視されます)。
- /A - 定義された IP アドレスまたはドメイン・ネームへの接続のみを許可する。
- /IP - 指定された ip_address への接続のみを許可する。
- /DN - 指定された domain_name (DNS 名) への接続のみを許可する。
- /NM - net_mask (オプション) デフォルト = 255.255.255.255

NETWK: NETWK コマンドは、すべてのネットワークの動作を制御します。

- NETWK /D は、すべてのネットワーク・アダプターを無効にして、すべてのネットワーク・トラフィックを無効にします。
- NETWK /E は、すべてのネットワーク・トラフィックを有効にします。ネットワークは、NETWK /E (有効) コマンドが実行されるまで無効になります。
- NETWK /A は、ネットワークを IP アドレスに制限します。IP アドレスは /IP スイッチ (ドット「.」付き 10 進数) または /DN (DNS 名) によって指定されます。
- NETWK /NM は、ネットワーク・マスクを提供します。/NM が提供されていない場合は、/IP または /DN によって指定された単一 PC のみがアクセス可能になります。このコマンドの状態は再起動されても存続するので、ネットワークは明示的に有効にする必要があります。

/NM スイッチはネットワーク・マスクを提供します。/NM が提供されていない場合は、/IP または /DN によって指定された単一 PC のみがアクセス可能になります。このコマンドの状態は再起動されても存続するので、ネットワークは明示的に有効にする必要があります。

REBOOT: REBOOT コマンドを使用すると、管理者が作成したスクリプトによって PC を再起動できます。このコマンドの構文は次のとおりです。

reboot.exe [/rr | /win] [/wait | /f]

- /rr - 起動して Rescue and Recovery ワークスペースに入ります。
- /win - 即時に起動してオペレーティング・システムに入ります (デフォルト)。
- /wait - システムの再起動時に、起動して Rescue and Recovery ワークスペースまたはオペレーティング・システムに入ります。
- /f - PC にすぐに再起動するよう強制し、開いているアプリケーションをユーザーが閉じるのを許可しません。

第 8 章 指紋認証ユーティリティー

指紋コンソールは 指紋認証ユーティリティー・インストール・フォルダーから実行する必要があります。基本的な構文は FPRCONSOLE [USER | SETTINGS] です。USER コマンドまたは SETTINGS コマンドは、どの操作セットを使用するかを指定します。完全なコマンドは「fprconsole user add TestUser /FORCED」のようになります。コマンドがわからない場合やすべてのパラメーターが指定されていない場合は、短いコマンド・リストがパラメーターと共に表示されます。

指紋認証ユーティリティーおよびマネージメント コンソールをダウンロードするには、次のリンクを使用してください。

`http://www.ibm.com/jp/domino05/pc/download/download.nsf/jtechinfo/TVAN-FPRDL`

ユーザー固有コマンド

ユーザーの登録や編集を行う場合は、USER セクションを使用します。現行ユーザーが管理者権限を持っていない場合、コンソールの振る舞いは指紋認証ユーティリティーのセキュリティー・モードによって異なります。保護モード: どのコマンドも許可されません。簡易モード: 標準ユーザーでは、ADD、EDIT、および DELETE コマンドが使用できます。ただし、ユーザーは自分のパスポート (ユーザー名で登録) しか変更できません。構文は次のとおりです。

FPRCONSOLE USER *command*

このとき、*command* は次のコマンドの 1 つです: ADD、EDIT、DELETE、LIST、IMPORT、EXPORT。

表 32.

コマンド	**構文**	**説明**	**例**
新規ユーザーの登録	ADD [*username* [| *domain¥username*]] [/FORCED]	/FORCED フラグによってウィザードのキャンセル・ボタンは使用不可になるので、登録は必ず正常に終了する必要があります。ユーザー名が指定されない場合は、現行ユーザー名が使用されます。	fprconsole add domain0¥testuser fprconsole add testuser fprconsole add testuser /FORCED
登録ユーザーの編集	EDIT [*username* [| *domain¥username*]]	ユーザー名が指定されない場合は、現行ユーザー名が使用されます。 **注:** 登録されるユーザーはまず自分の指紋を検査する必要があります。	fprconsole edit domain0¥testuser fprconsole edit testuser

表 32. (続き)

コマンド	構文	説明	例
ユーザーの削除	DELETE [*username* [| *domain*¥ *username* | /ALL]]	/ALL フラグは、この PC に登録されているすべてのユーザーを削除します。ユーザー名が指定されない場合は、現行ユーザー名が使用されます。	fprconsole delete domain0¥testuser fprconsole delete testuser fprconsole delete /ALL
登録ユーザーの列挙	List	登録されたユーザーをリストします。	
登録ユーザーのファイルへのエクスポート	Syntax: EXPORT username [| domain¥username] file	このコマンドは、登録ユーザーをハードディスクのファイルにエクスポートします。ユーザーは次に、別の PC 上、またはユーザーが削除されている場合は同じ PC 上の IMPORT コマンドを使用してインポートできます。	
登録ユーザーのインポート	Syntax: IMPORT *file*	このコマンドは指定したファイルからユーザーをインポートします。 **注:** ファイル上のユーザーが同じ指紋を使用してすでに同じ PC に登録されている場合は、識別操作でどちらのユーザーが優先順位を持つかは保証されません。	

グローバル設定のコマンド

指紋認証ユーティリティーのグローバル設定は、SETTINGS セクションによって変更できます。このセクションのすべてのコマンドには、管理者権限が必要です。構文は次のとおりです。

```
FPRCONSOLE SETTINGS command
```

このとき、*command* は次のコマンドの 1 つです: SECUREMODE、LOGON、CAD、TBX、SSO。

表 33.

コマンド	構文	説明	例
セキュリティー・モード	SECUREMODE 0|1	この設定は、指紋認証ユーティリティーの簡易モードと保護モードを切り替えます。	簡易モードの設定は次のようにします。 fprconsole settings securemode 0

表 33. (続き)

コマンド	構文	説明	例
ログオン・タイプ	LOGON 0|1 [/FUS]	この設定は、ログオン・アプリケーションを使用可能 (1)、または使用不可 (0) にします。 /FUS パラメーターを使用する場合、PC の構成上可能であれば、ユーザーの簡易切り替えモードでログオンが可能です。	
CTRL+ALT+DEL メッセージ	CAD 0|1	この設定は、ログオンでの「Ctrl+Alt+Delete を押す」テキストを使用可能 (1)、または使用不可 (0) にします。	
パワーオン・セキュリティー	TBX 0|1	この設定は、指紋認証ユーティリティーのパワーオン・セキュリティー・サポートをグローバルにオフ (0) にします。パワーオン・セキュリティー・サポートがオフになっている場合は、BIOS 設定に関係なく、パワーオン・セキュリティー・ウィザードやパワーオン・セキュリティー・ページは表示されません。	
パワーオン・セキュリティー・シングル・サインオン	SSO 0|1	この設定は、ユーザーが BIOS で検査された際に、自動的にユーザーをログオンさせるための logon で、BIOS で使用される指紋を使用可能 (1)、または使用不可 (0) にします。	

保護モードおよび簡易モード

ThinkVantage 指紋認証ユーティリティーは、保護モードと簡易モードの 2 つのセキュリティー・モードで実行することができます。

保護モードは、より高レベルのセキュリティーが必要な状況を対象としています。特定の機能は管理者にのみ、確保されています。追加認証をせず、パスワードを使用してログオンできるのは管理者だけです。

簡易モードは高レベルのセキュリティーをそれほど重要視しない、家庭用 PC を対象にしています。すべてのユーザーは、他のユーザーのパスポートの編集およびパスワードを使用して (指紋認証は行わない) システムにログオンするなどの、すべての操作を実行できます。

管理者 は、ローカル管理者グループの任意のメンバーです。保護モードを設定した後は、管理者だけが簡易モードに切り替えることができます。

保護モード - 管理者

セキュリティーを強化するために、ログオンのとき、誤ったユーザー名やパスワードが入力された場合は、保護モードでは次のメッセージが表示されます。「ユーザー名とパスワードでこの PC にログオンできるのは管理者だけです。」

表 34.

指紋	**説明**
新規パスポートの作成	管理者は自分のパスポートを作成することができ、また、制限ユーザーのパスポートも作成することができます。
パスポートの編集	管理者は自分のパスポートだけ を編集できます。
パスポートの削除	管理者はすべての制限ユーザーとその他の管理者のパスポートを削除できます。他のユーザーがパワーオン・セキュリティーを使用している場合、管理者はパワーオン・セキュリティーからユーザー・テンプレートをオプションで削除することができます。
パワーオン・セキュリティー	管理者は、パワーオンで使用される制限ユーザーおよび管理者の指紋を削除することができます。 **注:** パワーオン・モードが使用可能な場合は、少なくとも 1 つの指紋がなければなりません。
設定	
ログオン設定	管理者はすべてのログオン設定を変更できます。
保護スクリーン・セーバー	管理者はアクセスできます。
パスポート・タイプ	管理者はアクセスできます - サーバーと関連ある場合のみです。
セキュリティー・モード	管理者は保護モードと簡易モードを切り替えることができます。
Pro サーバー	管理者はアクセスできます - サーバーと関連ある場合のみです。

保護モード - 制限ユーザー

Windows にログオン中は、制限ユーザーはログオンに指紋を使用する必要があります。制限ユーザーの指紋センサーが作動していない場合は、管理者は指紋認証ユーティリティーの設定を簡易モードに変更して、ユーザー名とパスワードによるアクセスを可能にする必要があります。

表 35.

設定	**説明**
新規パスポートの作成	制限ユーザーはアクセスできません。
パスポートの編集	制限ユーザーは自分のパスポートだけを編集できます。

表 35. (続き)

設定	説明
パスポートの削除	制限ユーザーは自分のパスポートだけを削除できます。
パワーオン・セキュリティー	制限ユーザーはアクセスできません。
ログオン設定	制限ユーザーはログオン設定を変更できません。
保護スクリーン・セーバー	制限ユーザーはアクセスできます。
パスポート・タイプ	制限ユーザーはアクセスできません。
セキュリティー・モード	制限ユーザーはセキュリティー・モードを変更できません。
Pro サーバー	制限ユーザーはアクセスできます - サーバーと関連ある場合のみです。

簡易モード - 管理者

Windows へのログオン中は、管理者はユーザー名とパスワードを使用しても、指紋を使用してもログオンでき

表 36.

設定	説明
新規パスポートの作成	管理者は自分のパスポートだけ を作成できます。
パスポートの編集	管理者は自分のパスポートだけ を編集できます。
パスポートの削除	管理者は自分のパスポートだけ を削除できます。
パワーオン・セキュリティー	管理者は、パワーオンで使用される制限ユーザーおよび管理者の指紋を削除することができます。 **注:** パワーオン・モードが使用可能な場合は、少なくとも 1 つの指紋がなければなりません。
ログオン設定	管理者はすべてのログオン設定を変更できます。
保護スクリーン・セーバー	管理者はアクセスできます。
パスポート・タイプ	管理者はアクセスできます - サーバーと関連ある場合のみです。
セキュリティー・モード	管理者は保護モードと簡易モードを切り替えることができます。
Pro サーバー	管理者はアクセスできます - サーバーと関連ある場合のみです。

簡易モード - 制限ユーザー

Windows へのログオン中は、制限ユーザーはユーザー名とパスワードを使用しても、指紋を使用してもログオンできます。

表 37.

設定	説明
新規パスポートの作成	制限ユーザーは自分のパスワードだけを作成できます。
パスポートの編集	制限ユーザーは自分のパスポートだけを編集できます。
パスポートの削除	制限ユーザーは自分のパスポートだけを削除できます。
パワーオン・セキュリティー	制限ユーザーは自分の指紋だけを削除できます。
ログオン設定	制限ユーザーはログオン設定を変更できません。
保護スクリーン・セーバー	制限ユーザーはアクセスできます。
パスポート・タイプ	制限ユーザーはアクセスできません - サーバーと関連ある場合のみです。
セキュリティー・モード	制限ユーザーはセキュリティー・モードを変更できません。
Pro サーバー	制限ユーザーはアクセスできます - サーバーと関連ある場合のみです。

ThinkVantage 指紋認証ユーティリティーおよび Novell Netware Client

競合を防止するために、ThinkVantage 指紋認証ユーティリティーおよび Novell NetWare Client のユーザー名とパスワードは一致する必要があります。お使いの PC に ThinkVantage 指紋認証ユーティリティーがインストールしてあり、Novell Netware Client をインストールする場合は、レジストリーの一部の項目が上書きされることがあります。 ThinkVantage 指紋認証ユーティリティーのログオンで問題が発生した場合は、ログオン設定画面に移動して、ログオン・プロテクターを再度使用可能にしてください。

お使いの PC に Novell Netware Client がインストールされているが、ThinkVantage 指紋認証ユーティリティーのインストール前にクライアント PC にログオンしていなかった場合、Novell のログオン画面が表示されます。画面で、必要な情報を入力してください。

ログオン・プロテクター設定を変更するには、次のようにします。

- 「コントロールセンター」を開始する。
- 「**設定**」をクリックする。
- 「**ログオン設定**」をクリックする。
- ログオン・プロテクターを使用可能または使用不可にする。

指紋ログオンを使用したい場合は、「Windows ログオン認証を通常のパスワード認証から指紋認証に置き換える」チェック・ボックスにチェック・マークをつけます。

注: ログオン・プロテクターを使用可能、または使用不可にするには、再起動が必要です。

- お使いのシステムでユーザーの簡易切り替えがサポートされている場合は、これを使用可能または使用不可にする。
- (オプション機能) パワーオン・セキュリティーによって認証されたユーザーの自動ログオンを使用可能または使用不可にする。
- Novell ログオン設定を設定する。Novell ネットワークにログオンする場合は、次の設定が使用可能です。
  - **活動化**

    ThinkVantage 指紋認証ユーティリティーは自動的に既知のクレデンシャルを提供します。 Novell のログオンが失敗すると、Novell Client ログオン画面が表示され、正しいデータの入力を要求するプロンプトが出されます。
  - **ログオン中の質問**

    ThinkVantage 指紋認証ユーティリティーは Novell Client ログオン画面を表示して、ログオン・データの入力を要求するプロンプトを出します。
  - **使用不可**

    ThinkVantage 指紋認証ユーティリティーは Novell ログオンを試行しません。

第 9 章 ベスト・プラクティス

この章では、Rescue and Recovery、Client Security Solution、および指紋認証ユーティリティーのベスト・プラクティスを示すシナリオを提示します。このシナリオでは、ハードディスク・ドライブの設定から始まり、何回かの更新を行い、デプロイメントまでの手順を説明しています。 Lenovo および Lenovo 以外の両方の PC でのインストールを説明します。

Rescue and Recovery および Client Security Solution のインストールのデプロイメント例

次のセクションでは、Rescue and Recovery および Client Security Solution を、デスクトップとノートブックの両方にインストールする場合の例をいくつか挙げます。

デプロイメント・シナリオ 1

このセクションでは、今後発売される Lenovo および IBM ブランドの PC への Rescue and Recovery のインストールについて説明します。

ハードディスク・ドライブの準備

システムをデプロイする際にまず最初にすべきことは、ドナー・システムのハードディスク・ドライブを準備することです。新規ハードディスクを使用してデプロイを行う場合、ハードディスクのマスター・ブート・レコードをきれいにする必要があります。

1. Windows をインストールするハードディスク以外のすべてのストレージ・デバイス (セカンド・ハードディスク、USB ハードディスク、USB メモリー・キー、PC カード・メモリーなど) はドナー・システムから取り外しておいてください。

   重要: 以下のコマンドを実行すると、ターゲット・ハードディスク・ドライブの内容全体が消去されます。実行した後は、いかなるデータもターゲット・ハードディスク・ドライブからリカバリーすることができなくなります。
2. DOS 起動ディスケットを作成して、そのディスケットに cleandrv.exe ファイルを入れます。
3. そのディスケットを起動します。DOS プロンプトで、次のコマンドを入力します。

   ```
   CLEANDRV /HDD=0
   ```
4. ドナー・システムにオペレーティング・システムおよびアプリケーションをインストールします。ドナー・システムには、 Rescue and Recovery をインストールしないようにします。最後のステップで、Rescue and Recovery のインストールを行います。

インストール

最初に、InstallShield 形式の実行ファイル .EXE ファイルを C:¥RRTEMP フォルダーに解凍します。Rescue and Recovery を複数の PC にインストールする場合、このコマンドを 1 回行うことにより、各 PC のインストール時間が約半分に短縮されます。

1. インストール・ファイルが C ドライブのルートに置かれていることを前提として、ファイル EXE_EXTRACT.cmd を作成します。これは、ファイル C:¥SETUP_TVTRNR_*XXXX*.exe (ここで、*XXXX* はビルド ID です) を C:¥RRTEMP フォルダーに解凍するスクリプト・ファイルです。

```
:: This package will extract the WWW EXE to the directory c:¥RRTemp for an
:: administrative installation.
@ECHO OFF
:: This is the name of the EXE (Without the .EXE)
set BUILDID=setup_tvtrnr_xxxx.exe
:: This is the drive letter for the setu_tvtrnr_xxxx.exe
:: NOTE: DO NOT END THE STRING WITH A "¥".  IT IS ASSUMED TO NOT BE THERE.
SET SOURCEDRIVE=C:
:: Create the RRTemp directory on the HDD for the exploded WWW EXMD c:¥RRTemp
:: Explode the WWW EXE to the directory c:¥RRTemp
:: Note: The rnrdeploy.xml file must be copied into the same directory as the
:: MSIEXE file.
start /WAIT %SOURCEDRIVE%¥%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:¥RRTemp"
Copy Z180ZAB1011US00.tvt and Z333ZAA1001US00.tvt to C:¥rrtemp¥
```

2. Rescue and Recovery のインストールの前に多くのカスタマイズを行うことができます。以下に、いくつかの例を示します。
   - 増分バックアップの最大数を 4 に変更する。
   - Rescue and Recovery が毎日午後 1:59 に「Scheduled」というラベル名で、ローカル・ハードディスクに増分バックアップを取るように設定する。
   - Rescue and Recovery ユーザー・インターフェースを、ローカル管理者グループに属していないすべてのユーザーから隠す。
3. デフォルトの rnrdeploy.xml ファイルをカスタマイズします。一部のパラメーターは変更できます。詳しくは、145 ページの『付録 B. Rescue and Recovery のカスタマイズ』を参照してください。
4. カスタムの rnrdeploy.xml ファイルと同じフォルダーに install.cmd ファイルを作成します。これは、以下のアクションを実行します。
   - カスタムの rnrdeploy.xml ファイルを C:¥RRTemp フォルダーに作成されたインストール・パッケージにコピーします。
   - インストール後に再起動を行わない Rescue and Recovery のサイレント・インストールを実行します。
   - Rescue and Recovery を起動して、基本バックアップを実行します。
   - サービスが開始されたら、Rescue and Recovery CD の ISO イメージを作成する環境をセットアップします (これは通常、再起動の一部として実行されます)。
   - ISO イメージを作成します。
   - 基本バックアップを作成し、PC を再起動します。
5. install.cmd コードを変更します。以下に install.cmd のコードを示します。

```
:: Copy custom rnrdeploy.xml here
copy rnrdeploy.xml "c:¥RRTemp¥Program Files¥Lenovo¥Rescue and Recovery"
:: Install using the MSI with no reboot (Remove "REBOOT="R"" to force a reboot)
start /WAIT msiexec /i "c:¥TVTRR¥Rescue and Recovery - client security
  solution.msi" /qn REBOOT="R"
:: Start the service.  This is needed to create a base backup.
start /WAIT net start "Rescue and Recovery Service"
:: Make an ISO file here - ISO will reside in c:¥Program Files¥Lenovo¥Rescue and
Recovery¥rrcd
```

注: Rescue and Recovery のインストール後に PC を再起動する場合、以下の環境変数の設定は不要です。

```
:: Set up the environment
set PATH=%PATH%;%SystemDrive%¥Program Files¥Lenovo¥Common¥Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%¥Program Files¥Lenovo¥Common¥Python24
¥tcl¥tcl8.4
set TK_LIBRARY=%SystemDrive%¥Program Files¥Lenovo¥Common¥Python24
¥tcl¥tk8.4
set PYTHONCASEOK=1
set RR=C:¥Program Files¥Lenovo¥Rescue and Recovery¥
set PYTHONPATH=C:¥Program Files¥Lenovo¥Common¥logger
:: The next line will create the ISO silently and not burn it
C:¥Program Files¥Lenovo¥Common¥Python24¥python C:¥Program Files¥IBM
ThinkVantage¥Common¥spi¥mkspiim.pyc /scripted
:: Take the base backup... service must be started
c:
cd "C:¥Program Files¥Lenovo¥Rescue and Recovery"
RRcmd.exe backup location=L name=Base level=0
:: Reboot the system
C:¥Program Files¥Lenovo¥Common¥BMGR¥bmgr32.exe /R
```

更新

Windows に Service Pack を適用するなど、PC に大規模な変更を加える必要があることがあります。Service Pack をインストールする前に、PC で増分バックアップを作成しておき、そのバックアップにラベルを付けることができます。以下のステップを実行します。

1. FORCE_BU.CMD ファイルを作成して、そのファイルをターゲット・システムに配信します。
2. FORCE_BU.CMD ファイルがターゲット・システムに置かれたら、それを起動します。

以下に FORCE_BU.CMD ファイルの内容を示します。

```
:: Force a backup now
"%RR%rrcmd" backup location=L name="Backup Before XP-SP2 Update"
```

Rescue and Recovery デスクトップの有効化

次に、Rescue and Recovery ワークスペースの利点を活用しましょう。説明のため、次のセクションでは、Rescue and Recovery ワークスペースの制御ファイルを取得し、ユーザーが編集してから、rrutil.exe を使用して元の Rescue and Recovery ワークスペースに戻すことができるサンプルの UPDATE_RRE.CMD スクリプトを示します。詳しくは、 19 ページの『RRUTIL.EXE の使用』を参照してください。

Predesktop Area を変更するため、UPDATE_RRE.CMD スクリプトはいくつかの手順を明示します。

- rrutil.exe を使用して、Rescue and Recovery ワークスペースからファイルを取得します。 Rescue and Recovery ワークスペースから取得するファイルは、ファイル getlist.txt で定義されます。
- 適切なファイルを編集した後、ファイルを元の Rescue and Recovery ワークスペースを戻すためのフォルダー構造を作成しておきます。
- 保存して編集するために、ファイルのコピーを作成します。

この例では、エンド・ユーザーが Rescue and Recovery ワークスペースで「**ブラウザーを開く**」ボタンをクリックすると開かれるホーム・ページを変更します。 Web ページ `http://www.ibm.com/jp/pc/think/thinkvantagetech/` (英語のサイトです) が開きます。

変更を行うには、Notepad で pdaguien.ini ファイルを開いて、

1. 下記のように行を変更します。

   ```
   button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
   %sysdrive%¥Preboot¥Opera¥Opera.EXE, http://www.pc.lenovo.com/cgi-
   bin/access_IBM.cgi?version=4&link=gen_support&country=__
   COUNTRY__&language=__LANGUAGE__
   ```

   から次のように変更します。

   ```
   button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
   %sysdrive%¥Preboot¥Opera¥Opera.EXE,
    http://www.ibm.com/jp/pc/think/thinkvantagetech/
   ```
2. ファイルを Rescue and Recovery ワークスペースに配置するために用意したフォルダーにコピーします。詳しくは、 19 ページの『RRUTIL.EXE の使用』を参照してください。
3. PC を再起動して Rescue and Recovery ワークスペースに入ります。
4. システムを分析して、バックアップする必要があるファイルがあることを判別したら、HKLM¥SOFTWARE¥Lenovo¥Rescue and Recovery¥Settings¥BackupList のレジストリー・キーを更新します。

表 38. UPDATE_RR.CMD script

```
@ECHO OFF
::Obtain the PDAGUIen.ini file from the RR
c:¥RRDeployGuide¥RRUTIL¥RRUTIL -g getlist.txt
c:¥RRDeployGuide¥GuideExample¥RROriginal
:: Make a directory to put the edited file for import back into the RR
md c:¥RRDeployGuide¥GuideExample¥put¥preboot¥usrintfc
:: Open the file with notepad and edit it.
ECHO.
ECHO Edit the file
c:¥RRDeployGuide¥GuideExample¥RROriginal¥PDAGUIen.ini
```

File will open automatically

```
pause
:: Make a copy of original file
copy
c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥PDAGUIen.ini
c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥
PDAGUIen.original.ini
notepad
c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥PDAGUIen.ini
pause
copy c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥
PDAGUIen.ini c:¥RRDeployGuide¥GuideExample¥put¥preboot¥usrintfc
:: Place the updated version of the PDAGUIen into the RR
c:¥RRDeployGuide¥RRUTIL¥RRUTIL -p c:¥RRDeployGuide¥GuideExample¥put
ECHO.
ECHO Reboot to the RR to see the change
pause
c:¥Program Files¥Lenovo¥Common¥BMGR¥bmgr32.exe /bw /r
```

Create getlist.txt:

```
¥preboot¥usrintfc¥pdaguien.ini
```

デプロイメント・シナリオ 2

このセクションでは、OEM PC への Rescue and Recovery のインストールについて説明します。Rescue and Recovery をインストールするには、ハードディスク上のマスター・ブート・レコードで先頭の 8 セクターがブランクである必要があります。Rescue and Recovery は、リカバリー領域に入るためにカスタム・ブート・マネージャーを使用します。

マスター・ブート・レコードを使用する一部の他社製アプリケーションでは、製品のポインターがマスター・ブート・レコード・セクターに保存されます。このポインターが Rescue and Recovery のブート・マネージャーのインストールに干渉する場合があります。

下記のシナリオとベスト・プラクティスを参考にして、Rescue and Recovery により確実に望ましい機能が提供されるようにしてください。

ハードディスク・ドライブのセットアップのベスト・プラクティス: オプション 1

このシナリオでは、Rescue and Recovery を含む新規イメージのデプロイメントを扱います。Rescue and Recovery を マスター・ブート・レコードを使用するアプリケーションがインストールされたクライアント PC にデプロイするには、下記のテストを行って、Rescue and Recovery に干渉するかどうかを判別します。

1. テスト・クライアント PC をセットアップする。
2. Rescue and Recovery をインストールします。マスター・ブート・レコード (MBR) を使用する他のアプリケーションがあるために MBR の先頭 8 セクターに空きがない場合、次のエラー・メッセージが表示されます。

```
Error 1722. There is a problem with this Windows
Installer package. A program run as part of the
setup did not finish as expected. Contact your
personnel or package vendor.
```

基本オペレーティング・システムに OEM イメージを使用している場合、マスター・ブート・レコード に製品リカバリー・データが含まれていないことを確認してください。これは次の方法で行うことができます。

重要: 次のコマンドを実行すると、ターゲット・ハードディスク・ドライブの内容全体が消去されます。実行した後は、いかなるデータもターゲット・ハードディスク・ドライブからリカバリーすることができなくなります。

1. 以下のサイトから cleandrv.exe を入手する。

   `http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN`
   (英語のサイトです)

   基本イメージの作成に使用するハードディスク・ドライブ上のマスター・ブート・レコードからすべてのセクターが消去されていることを確認する。
2. Windows をインストール後、ガイドに従ってイメージを作成する。

ハードディスク・ドライブのセットアップのベスト・プラクティス: オプション 2

Rescue and Recovery を既存のクライアント PC にデプロイするには、多少の努力と計画が必要です。このシナリオでは、ハードディスク・セットアップの別のオプションについて説明します。

注: エラー 1722 を受け取り、8 つの空きセクターを作成する必要がある場合、スマートセンターに連絡してエラーを報告し、さらなる指示を要請してください。

Rescue and Recovery の起動可能 CD の作成: Rescue and Recovery ワークスペースを起動することができるレスキュー・メディア CD は、あらかじめ作成されている ISO イメージを展開するのではなく、現在のサービス区画の内容から作成します。ただし、適切な ISO (.iso) イメージが以前に作成され、すでに存在する場合は、新しい ISO イメージを作成するのではなく、その ISO イメージを CD に書き出します。

ISO イメージの作成、CD への書き出しを行う場合、他のアプリケーションの起動を行わないようにしてください。これらの作業中に他のアプリケーションを実行すると、アプリケーションが強制終了することがあります。また、スクリーンセーバーや省電力設定も無効にしておくことを推奨いたします。ハードディスク・ドライブの保護領域へのアクセスの性質上、管理者のみが ISO を作成することができます。以下のファイルおよびフォルダーは、レスキュー・メディアに組み込まれます。

- minint

- preboot
- win51
- win51ip
- win51ip.sp1
- scrrec.ver

注: 新規 ISO イメージを作成する場合、上記のフォルダー・ファイルをコピーし、ISO をビルドするために、システム・ドライブに最低 400 MB の空き容量が必要です。この容量のデータを移動するのはハードディスク・ドライブに負担がかかるタスクであるため、PC によっては 15 分以上かかる場合があります。

ISO ファイルの作成および CD サンプル・スクリプト・ファイルへの書き出し: ISO ファイルを作成して、CD サンプル・スクリプト・ファイルに書き出すには、次のコードを準備します。

```
:: Make an ISO file here - ISO will reside in c:¥SWTOOLS¥rrcd
```

注: 以下の 7 行のコード (Bold フォントで表示) は、Rescue and Recovery のインストール後に再起動を行っていない場合にのみ必要です。

```
:: Set up the environment

set PATH=%PATH%;%SystemDrive%¥Program Files¥Lenovo¥Common¥Python24

set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY

set TCL_LIBRARY=%SystemDrive%¥Program Files¥Lenovo¥Common¥Python24
¥tcl¥tcl8.4

set TK_LIBRARY=%SystemDrive%¥Program Files¥Lenovo¥Common¥Python24
¥tcl¥tk8.4

set PYTHONCASEOK=1

set RR=c:¥Program Files¥Lenovo¥Rescue and Recovery¥

set PYTHONPATH=C:¥Program files¥Lenovo¥Common¥logger

:: The next line will create the ISO silently and not burn it

c:¥Program Files¥Lenovo¥Common¥Python24¥python c:¥Program Files¥
Lenovo¥Common¥spi¥mkspiim.pyc /scripted

:: The next line will create the ISO with user interaction and not burn it

:: c:¥Program Files¥Lenovo¥Common¥Python24¥python c:¥Program Files¥
Lenovo¥Common¥spi¥mkspiim.pyc /scripted

/noburn
```

デプロイメント・シナリオ 3

これは、各製品を次のような仮定のカスタマー要件でデスクトップ PC にインストールする場合の例です。

- **Administration**
  - Rescue and Recovery を使用して Sysprep の基本バックアップを作成
  - PC の管理にローカル管理者アカウントを使用
- **Rescue and Recovery**
  - Client Security のパスフレーズを使用して Rescue and Recovery ワークスペースへのアクセスを保護

– マスター・パスワードが基本バックアップにすでに設定されているので、Windows パスワードを促すプロンプトが非表示
– ログオン提供 (GINA)
– 指紋認証ユーティリティーをインストールし、Windows とワークスペースの両方のログオンに使用

- **Client Security Solution**
  – エミュレーション・モードでのインストールおよび実行
    - IBM または Lenovo の PC は、すべてが TPM (セキュリティー・チップ) を備えているわけではありません。
  – Password Manager 非搭載
    - 代わりに企業向けシングル・サインオン・ソリューションを使用します。
  – Client Security パスフレーズを使用可能に設定
    - パスフレーズによって Client Security Solution アプリケーションを保護します。
  – Client Security Windows ログオンを使用可能に設定
    - Client Security パスフレーズで Windows にログインします。
  – すべてのユーザーに 500 MB の SafeGuard PrivateDisk を作成
    - 各ユーザーには、データを安全に保管するために 500 MB のスペースが必要です。
  – エンド・ユーザー・パスフレーズのリカバリー機能を使用可能に設定
    - ユーザーが、自分で決めた 3 つの質問に答えることによって、パスフレーズをリカバリーできるようにします。
  – Client Security Solution XML スクリプトをパスワード = “XMLscriptPW” で暗号化
    - パスワードによって、Client Security Solution 構成ファイルを保護します。
  – 指紋認証ユーティリティーのインストールはオプション

準備 PC で以下を実行します。

1. 「ローカル管理者」アカウントで Windows にログインします。
2. Rescue and Recovery および Client Security Solution プログラムを、次のオプションを指定してインストールします。

```
For Rescue and Recovery:
setup_tvtrnr_xxxx.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
(where XXXX is the build ID)
"NOCSSWIZARD=1""
```

```
Client Security Solution の場合:
setup_tvtcss_xxxx.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
(where XXXX is the build ID)
"NOCSSWIZARD=1""
```

注:

a. XML ファイル (rnrdeploy.xml など) が実行可能ファイルと同じフォルダーにあることを確認します。同じフォルダーにない場合、インストールは失敗します。
b. 管理者インストールを実行する場合は、125 ページの『デプロイメント・シナリオ 1』を参照してください。

3. 再起動後はローカル管理者アカウントで Windows にログインし、デプロイメント用の XML スクリプトを作成します。コマンド・ラインから次のコマンドを実行してください。

```
"C:¥Program Files¥Lenovo¥Client Security Solution¥css_wizarde.exe"
/name:C:¥ThinkCentre
```

ウィザードで、次のオプションを選択します。

- 「**拡張**」→「**次へ**」をクリック
- 「**Client Security パスフレーズ**」→「**次へ**」をクリック
- 「**Client Security ログイン画面を使用するログオン**」→「**次へ**」をクリック
- 管理者アカウント用の Windows パスワードを入力し、「**次へ**」をクリック

  (たとえば WPW4Admin)
- 管理者アカウント用の Client Security パスフレーズを入力し、「**Client Security パスフレーズを使用して、Rescue and Recovery ワークスペースへのアクセスを保護する**」ボックスにチェック・マークを付けて、「 **次へ**」をクリック

  (たとえば CSPP4Admin)
- パスワードまたはパスフレーズの復元についての質問の選択画面が開きます。管理者アカウント用の 3 つの質問と回答を選択してから、「**次へ**」をクリック
  a. 初めて飼ったペットの名前は?

     (たとえば Snowball)
  b. 好きな映画は?

     (たとえば『風と共に去りぬ』)
  c. 好きなスポーツ・チームは?

     (たとえば Carolina Panthers)
- 「**各ユーザーの暗号化 PrivateDisk ドライブを、選択された次の形式で作成します。**」のチェックを外し、「**次へ**」をクリック
- 「要約」を確認し、「**適用**」を選択して XML ファイルを C:¥ThinkCentre.xml に書き込み、もう一度「**適用**」をクリック
- 「**完了**」をクリックしてウィザードを閉じる

4. テキスト・エディターで次のファイルを開き (XML スクリプト・エディターまたは Microsoft Word 2003 には XML フォーマット機能が組み込まれています)、以下の設定を変更します。
   - ドメイン設定への参照をすべて削除します。これにより、スクリプトには、各システムで代わりにローカル PC 名を使用するように通知されます。ファイルを保存します。
5. C:¥Program Files¥Lenovo¥Client Security Solution¥xml_crypt_tool.exe のツールを使用して、XML スクリプトをパスワードで暗号化します。コマンド・プロンプトからファイルを実行するには、次の構文を使用します。
   a. xml_crypt_tool.exe C:¥ThinkCentre.xml /encrypt XMLScriptPW.

b. これでファイルは C:¥ThinkCentre.xml.enc となり、パスワード = XMLScriptPW で保護されます。

これで、ファイル C:¥ThinkCentre.xml.enc をデプロイメント PC に追加する準備ができました。

デプロイメント PC で以下を実行します。

1. ローカル管理者アカウントで Windows にログインします。
2. Rescue and Recovery および Client Security Solution プログラムを、次のオプションを指定してインストールします。

```
setup_tvtrnr_xxxx.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
(where XXXX is the build ID)
"NOCSSWIZARD=1""
```

注:

a. .tvt ファイル (z062zaa1025us00.tvt など) が実行可能ファイルと同じフォルダーにあることを確認します。同じフォルダーにない場合、インストールは失敗します。

b. 管理用インストールを実行する場合は、 125 ページの『デプロイメント・シナリオ 1』を参照してください。

3. 再起動後、ローカル管理者アカウントで Windows にログインします。
4. 先に作成した ThinkCentre™.xml.enc ファイルを C:¥ のルート・ディレクトリーに追加します。
5. レジストリーを変更して、全ユーザーでデフォルトの SafeGuard PrivateDisk Volume Size = 500 MB を設定します。これは、*reg* ファイルをインポートすると簡単にできます。

   a. HKEY_LOCAL_MACHINE¥SOFTWARE¥Lenovo¥Client Security Software に移動します。

   b. 新規のストリング値 (値の名前: = PrivateDiskSize、値のデータ: = 500) を作成します。

   c. DWORD 値 (値の名前: = UsingPrivateDisk、値のデータ: = 1) を作成します。

6. RunOnceEx コマンドを、以下のパラメーターを指定して作成します。
   - RunonceEx キーに「0001」という新規キーを追加します。次のようになります。 HKEY_LOCAL_MACHINE ¥Software¥Microsoft¥Windows¥Current Version¥RunOnceEx¥0001
   - そのキーに、ストリング値の名前 「CSSEnroll」を次の値で追加します。 ″C:¥Program Files¥Lenovo¥Client Security Solution¥vmservere.exe” C:¥ThinkCenter.xml.enc XMLscriptPW
7. “%rr%¥rrcmd.exe sysprepbackup location=L name=”Sysprep Backup” を実行します。システムの準備ができたら、次のように出力されます。

```
*******************************************************
** Ready to take sysprep backup.                     **
**                                                   **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.             **
**                                                   **
** Next time the machine boots, it will boot         **
** to the Predesktop Area and take a backup.         **
*******************************************************
```

8. Sysprep を実行します。
9. PC をシャットダウンしてから再起動します。Rescue and Recovery ワークスペースで、バックアップ処理が開始されます。

   注: メッセージ「復元が進行中ですが、バックアップが行われています (Restore in progress but a backup is occurring)」が表示されます。バックアップ後は、電源をオフにします。再起動はしないでください。

これで、Sysprep の基本バックアップが完了しました。

デプロイメント・シナリオ 4

これは、各製品を次のような仮定のカスタマー要件でノートブックにインストールする場合の例です。

- **Administration**
  - 以前のバージョンの Rescue and Recovery および Client Security Solution がインストールされている PC にインストール
  - PC の管理にドメイン管理者アカウントを使用
  - すべての PC に、BIOS スーパーバイザー・パスワード BIOSpw を割り当て
- **Client Security Solution**
  - TPM を活用
    - すべての PC にセキュリティー・チップを搭載
  - Password Manager を使用可能に設定
  - SafeGuard PrivateDisk を使用不可に設定
    - 代わりに、Utimaco SafeGuard Easy によるハードディスクの完全暗号化を使用します。
  - Client Security Solution に対する認証として、ユーザーの Windows パスワードを活用
    - Utimaco SafeGuard Easy、Client Security Solution、および Windows ドメインに対する認証で、単一の Windows パスワードを許可
  - Client Security Solution XML スクリプトを、パスワード = ″XMLscriptPW″ で暗号化
    - このパスワードによって、Client Security Solution 構成ファイルを保護します。
- **ThinkVantage 指紋認証ユーティリティー**
  - BIOS とハードディスクのパスワードを使用しない
  - 指紋認証ユーティリティーによるログオン
    - 一定のセルフ・ユーザー登録期間後、ユーザーは、非管理者ユーザーの場合は指紋を必要とするセキュア・モード・ログオンに切り替えるため、デュアル・ファクター認証方式を効果的に実行できます。
  - 指紋チュートリアルの組み込み
    - エンド・ユーザーが、指紋を正しく読み取らせる方法や、操作を間違った場合は視覚的なフィードバックを得る方法を知ることができます。

準備 PC で以下を実行します。

1. 電源オフの状態から PC を始動し、**F1** を押して BIOS に入り、「Security」メニューに移動して「Clear Security Chip」を「Yes」にします。保管してから BIOS を終了します。
2. ドメイン管理者アカウントで Windows にログインします。
3. ThinkVantage 指紋認証ユーティリティーをインストールします。f001zpz2001us00.exe を実行して、Web パッケージから setup.exe を解凍します。setup.exe は、自動的に C:¥SWTOOLS¥APPS¥TFS4.6-Build1153¥Application¥0409¥setup.exe に解凍されます。
4. f001zpz7001us00.exe を実行して Web パッケージから tutess.exe ファイルを解凍し、ThinkVantage 指紋チュートリアルをインストールします。setup.exe は、自動的に C:¥SWTOOLS¥APPS¥tutorial¥TFS4.6-Build1153¥Tutorial¥0409¥tutess.exe に解凍されます。
5. f001zpz5001us00.exe を実行して Web パッケージから fprconsole.exe を解凍し、ThinkVantage 指紋コンソールをインストールします。f001zpz5001us00.exe を実行すると、setup.exe は、自動的に C:¥SWTOOLS¥APPS¥fpr_con¥APPS¥UPEK¥FPR Console¥TFS4.6-Build1153¥Fprconsole¥fprconsole.exe に解凍されます。
6. Client Security Solution プログラムを、次のオプションを指定してインストールします。

```
setup_tvtcss_xxxx.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=
(where XXXX is the build ID)
"BIOSpw""
```

7. 再起動後はドメイン管理者アカウントで Windows にログインし、デプロイメント用の XML スクリプトを作成します。コマンド・ラインから次のコマンドを実行してください。

```
"C:¥Program Files¥Lenovo¥Client Security Solution¥css_wizard.exe"
/name:C:¥ThinkPad
```

   ウィザードで、スクリプト例に合わせて次のオプションを選択します。
   - 「**拡張**」→「**次へ**」をクリック
   - 「**Windows パスワード**」→「**次へ**」をクリック
   - 「**指紋を使用するログオン**」→「**次へ**」をクリック
   - 管理者アカウント用の Windows パスワードを入力し、「**次へ**」をクリック

     (たとえば WPW4Admin)
   - パスワードのリカバリーを有効にするためのチェックを外し、「**次へ**」をクリック
   - 要約を確認し、「**適用**」をクリックして、XML ファイルを C:¥ThinkPad.xml に書き込む
   - 「**完了**」をクリックしてウィザードを閉じる
8. C:¥Program Files¥Lenovo¥Client Security Solution¥xml_crypt_tool.exe のツールを使用して、XML スクリプトをパスワードで暗号化します。コマンド・プロンプトから、次の構文を実行します。

   a. xml_crypt_tool.exe C:¥ThinkPad.xml /encrypt XMLScriptPW.

b. これでファイルは C:¥ThinkPad.xml.enc となり、パスワード = XMLScriptPW で保護されます。

デプロイメント PC で以下を実行します。

1. 自社のソフトウェア配布ツールを使用して、ThinkVantage 指紋認証ユーティリティーの実行可能ファイル setup.exe (準備 PC から各デプロイメント PC に解凍されたもの) をデプロイします。setup.exe が PC に配信されたら、次のコマンドを実行してインストールを行います。

   ```
   setup.exe CTLCNTR=0 /q /i
   ```

2. 自社のソフトウェア配布ツールを使用して、ThinkVantage 指紋チュートリアルの実行可能ファイル tutess.exe (準備 PC から各デプロイメント PC に解凍されたもの) をデプロイします。tutess.exe が PC に配信されたら、次のコマンドを実行してインストールを行います。

   ```
   tutess.exe /q /i
   ```

3. 自社のソフトウェア配布ツールを使用して、ThinkVantage 指紋コンソールの実行可能ファイル fprconsole.exe (準備 PC から各デプロイメント PC に解凍されたもの) をデプロイします。
   - fprconsole.exe ファイルを C:¥Program Files¥ThinkVantage Fingerprint Software¥ フォルダーに入れます。
   - 次のコマンドを実行して、BIOS パワーオン・セキュリティー・サポートをオフにします。 fprconsole.exe settings TBX 0
4. 自社のソフトウェア配布ツールを使用して、Client Security Solution 実行可能ファイル「setup_tvtcss_xxxx.exe」(ここで、*XXXX* はビルド ID です) をデプロイします。
   - setup_tvtcss_xxxx.exe が PC に配信されたら、次のコマンドを実行してインストールを行います。setup_tvtcss_xxxx.exe /s /v/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=”BIOSpw”
   - ソフトウェアをインストールすると、 TPM ハードウェアが自動的に使用可能になります。
5. システムの再起動後、次の手順で、XML スクリプト・ファイルによるシステム構成を行います。
   - 先に作成した ThinkPad.xml.enc ファイルを C:¥ フォルダーにコピーします。
   - 別のコマンド・プロンプトを開き、以下を実行します。C:¥Program Files¥Lenovo¥Client Security Solution¥vmserver.exe C:¥ThinkPad.xml.enc XMLScriptPW
6. 再起動後は、システムで Client Security Solution ユーザー登録の準備ができています。各ユーザーは、それぞれのユーザー ID と Windows パスワードでシステムにログインできます。システムにログインするすべてのユーザーに、Client Security Solution への登録を促すプロンプトが自動的に出され、登録すると、指紋センサーへの登録ができるようになります。
7. システムのすべてのユーザーが ThinkVantage 指紋認証ユーティリティーに登録されたら、セキュア・モード設定を使用可能にして、Windows のすべての非管理者ユーザーに、各自の指紋でログオンさせるようにすることができます。
   - 次のコマンドを実行します。C:¥Program Files¥ThinkVantage 指紋認証ユーティリティー¥fprconsole.exe settings securemode 1

- メッセージを削除するには、Ctrl+Alt+Delete を押してパスワードでログオンします。ログオン画面で、次のコマンドを実行します。

```
C:¥Program Files¥ThinkVantage 指紋認証ユーティリティー¥fprconsole.exe settings
CAD 0
```

これで、Client Security Solution 7.0 と ThinkVantage 指紋認証ユーティリティーのデプロイメントが完了しました。

デプロイメント・シナリオ 5

このセクションでは、Rescue and Recovery のタイプ 12 サービス区画へのインストールについて説明します。Rescue and Recovery をタイプ 12 サービス区画にインストールするには、以下を用意する必要があります。
- SP.PQI ファイル。このファイルには、サービス区画を作成するための基本の起動可能ファイルが含まれています。
- PowerQuest PQDeploy
- Rescue and Recovery の最新インストーラー

Rescue and Recovery ワークスペースをサービス区画にインストールするには、いくつかの関連するオプションがあります。

注: タイプ 12 の区画は、Windows と同じドライブ上の区画テーブルで最後に使用された項目に置かれている必要があります。タイプ 12 の区画がハードディスクのどこにあるかは、BMGR32 の情報でわかります。詳しくは、190 ページの『Rescue and Recovery ブート・マネージャーの制御 (BMGR32)』を参照してください。

インストールを行うには、以下の手順を実行してください。
1. ドライブの最後に最小 700 MB の未割り当ての空き容量を残しておきます。
2. PowerQuest PQDeploy を使用して、SP.pqi ファイルを未割り当ての空き容量に復元します。PowerQuest PQDeploy に関する追加の支援が必要な場合は、PowerQuest の資料を参照してください。
3. ステップ 1 で作成した基本区画 (C ドライブを除く) を削除してから、再起動します。

   注: システム・ボリューム情報が新しく作成されたサービス区画に表示されます。システム・ボリューム情報は、Windows の「システムの復元」を「無効」に設定し、削除してください。

4. Rescue and Recovery をインストールし、再起動するようプロンプトが出たら、再起動します。

デプロイメント・シナリオ 6

次の例は、管理用テンプレート・ファイル (.adm) をローカルから使用できる方法、および設定値をレジストリー・ファイルを使用してエクスポートしてからすべての該当 PC にインポートできる方法を説明しています。この例では、メイン・ユーザー・インターフェースの「拡張」メニューを隠す方法について説明しています。
1. イメージ PC に Rescue and Recovery 3.1 をインストールします。
2. Windows の「スタート」メニューの「ファイル名を指定して実行」に gpedit.msc と入力します。

3. 「コンピュータの構成」の「管理用テンプレート」を右クリックします。
4. 「テンプレートの追加と削除」を選択します。
5. 「追加」ボタンを押してから、rnr.adm ファイルを選択します。rnr.adm ファイルは、
http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN (英語のサイトです) にある管理ツール・パッケージから入手できます。
6. 「テンプレートの追加と削除」ダイアログ・ボックスの「閉じる」ボタンを押します。
7. 「コンピュータの構成」の「管理用テンプレート」タブをクリックします。「ThinkVantage」という名前の新しいタブがあります。「ThinkVantage」タブの下に「Rescue and Recovery」タブがあります。これで、この PC 用に、すべての選択可能な設定を構成できます。
8. 「Thinkvantage」→「Rescue and Recovery」→「ユーザー・インターフェース (User Interface)」→「メニュー (Menus)」に進み、「拡張メニュー (Advanced Menu)」タブをダブルクリックします。
9. 「拡張メニューのプロパティ (Advanced Menu Properties)」ダイアログ・ボックスの「設定」タブで「有効」を選択します。
10. 「拡張メニュー (Advanced Menu)」のラベルが付いたドロップダウン・ボックスから「非表示 (Hide)」を選択します。
11. 「拡張メニューのプロパティ (Advanced Menu Properties)」ダイアログ・ボックスで「OK」をクリックします。
12. Windows の「スタート」メニューから regedit を実行します。
13. 次のレジストリー・キーにナビゲートして右クリックします。
HKLM¥Software¥Policies¥Lenovo¥Rescue and Recovery
14. 「エクスポート」をクリックします。
15. 「レジストリ ファイルの書き出し」ダイアログ・ボックスの「ファイル名」フィールドにファイル名を入力します。
16. 「レジストリ ファイルの書き出し」ダイアログ・ボックスの「保存する場所」フィールドで、対象とするパスにナビゲートします。
17. 「保存」ボタンを押します。

これで、Rescue and Recovery のサイレント・インストールを実行するインストール・パッケージを作成でき、パッケージがこの新しいレジストリー・キーをインポートして、すべての PC で拡張メニューを隠すようにすることができます。これは、ADM ファイルのすべての設定で使用できます。

Sysprep のバックアップ/復元

パスワードの保存は、Sysprep のバックアップ/復元では機能しません。Sysprep のバックアップが完了したら、電源をオフにし、システムを再起動してください。

Client Security Solution モードの切り替え

Client Security Solution モードを「便利なログオン・メソッド」から「セキュア・ログオン・メソッド」に切り替えるか、「セキュア・ログオン・メソッド」から「便

利なログオン・メソッド」に切り替える場合で、システムのバックアップに Rescue and Recovery を使用している場合、モードを切り替えた後に新しい基本バックアップをとってください。

Computrace と Rescue and Recovery

非 BIOS バージョンの Computrace がインストールされているシステムでは、Rescue and Recovery をアンインストールできません。

企業用 Active Directory のロールアウト

企業用 Active Directory をロールアウトする場合、次のステップを実行します。

1. Active Directory または LANDesk を使用してインストールします。
   a. Active Directory および LANDesk を使用してバックアップを取り、バックアップを取った人物と時点について報告を得ます。
   b. バックアップの作成、バックアップの削除、スケジュール・オプション、およびパスワードの制約事項に関する機能を特定のグループに付与してから、グループを変更し、設定が存続するかどうかを参照します。
   c. Active Directory から Antidote Delivery Manager を有効にします。実行するパッケージを提供し、報告が取り込まれることを確認します。

CD またはスクリプト・ファイルのスタンドアロン・インストール

CD またはスクリプト・ファイルのスタンドアロン・インストールの場合、次のステップを実行します。

1. バッチ・ファイルを使用して Rescue and Recovery、Client Security Solution、および指紋認証ユーティリティーをサイレント・インストールします。
2. BIOS パスワード・リカバリーをサイレント構成します。

システムの更新

システムを更新するには、次のステップを実行します。

1. 内容を制御するために、Lenovo サーバーに移動する代わりに、大企業がサーバーをセットアップする方法をシミュレートして、カスタマイズ済みのシステム更新サーバーを使って Rescue and Recovery、Client Security Solution、および指紋認証ユーティリティー・テクノロジーをインストールします。
2. 3 種類のバージョンの古いソフトウェア (Rescue and Recovery 1.0/2.0/3.0、指紋認証、Client Security Solution 5.4-6、FFE) を上書きインストールします。古いバージョンに宇和がs気して新しいバージョンをインストールする際には、設定を保持する必要があります。

System Migration Assistant

Rescue and Recovery 3.0 および Client Security Solution 6.0 のある T40 から、Rescue and Recovery 3.1 および Client Security Solution 7.0 のある T43 にマイグレーションします。

付録 A. インストール・コマンド・ライン・パラメーター

Microsoft Windows インストーラーは、コマンド・ライン・パラメーターによって、複数の管理機能を提供します。

管理用インストールの手順およびコマンド・ライン・パラメーター

Windows インストーラーは、ワークグループによる使用またはカスタマイズのために、アプリケーションまたは製品のネットワークへの管理用インストールを実行できます。Rescue and Recovery インストール・パッケージまたは Client Security Solution インストール・パッケージの場合、管理用インストールによりインストール・ソース・ファイルが指定された場所に解凍されます。

管理用インストールを実行するには、セットアップ・パッケージをコマンド・ラインから /a パラメーターを使用して実行します。

```
setup.exe /a
```

管理用インストールは、管理ユーザーにセットアップ・ファイルの解凍先を指定するようプロンプトを出すウィザードを表示します。デフォルトの解凍先は C:¥ です。C:¥ 以外のドライブ (その他のローカル・ドライブ、または割り当てられたネットワーク・ドライブなど) の新しい場所を選択することもできます。新しいフォルダーも、この手順で作成できます。

管理用インストールをサイレント・インストールで実行する場合、解凍先の場所を指定するために、コマンド・ラインで次のように共通プロパティ TARGETDIR を設定することができます。

```
setup.exe /s /v"/qn TARGETDIR=F:¥TVTRR"
```

注: setup.exe は、Windows インストーラーのバージョンが最新ではない場合に Windows インストーラー・エンジンをバージョン 3.0 に更新するように構成されています。この更新が行われると、管理用の解凍インストールの場合でも、インストール・アクションによって再起動のプロンプトが出されます。この状態での再起動を防止するために、再起動を適切に行ってください。Windows インストーラーが少なくともバージョン 3.0 である場合、setup.exe はインストールを試行しません。

または

```
msiexec.exe /i "Lenovo Rescue and Recovery.msi" /qn TARGERDIR=F:¥TVTRR
```

管理用インストールが完了した後、管理者はソース・ファイルをカスタマイズ (たとえば、レジストリーに設定値を追加) することができます。カスタマイズした後に解凍したソースからインストールするには、ユーザーはコマンド・ラインで msiexec.exe を実行し、解凍された MSI ファイルの名前を引き渡します。

msiexec.exe の使用

カスタマイズした後に解凍したソースからインストールするには、ユーザーはコマンド・ラインで msiexec.exe を実行し、解凍された *.MSI ファイルの名前を引き渡

します。msiexec.exe は、インストール・パッケージを解釈し、製品をターゲット PC にインストールするために使用するインストーラーの実行可能プログラムです。

```
msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥
Personal¥MySetups¥project name¥product configuration¥release name¥
DiskImages¥Disk1¥product name.msi"
```

注: 上記のコマンドを、円記号の後にスペースを入れずに 1 行として入力します。

表 39 は、msiexec.exe で有効なコマンド・ライン・パラメーターと、その使用方法を説明します。

表 39. コマンド・ライン・パラメーター

パラメーター	**説明**
/I *package* または *product code*	このフォーマットは製品のインストールに使用します。 `Othello:msiexec /i "C:¥WindowsFolder¥Profiles¥` `UserName¥Personal¥MySetups` `¥Othello¥Trial Version¥` `Release¥DiskImages¥Disk1¥` `Othello Beta.msi"` 製品コードとは、製品のプロジェクト・ビューの製品コード・プロパティで自動的に生成されるグローバル一意識別子 (GUID) のことです。
/a *package*	**/a** オプションにより、管理者権限を持つユーザーは製品をネットワーク上にインストールできます。
/x *package* または *product code*	**/x** オプションは、製品をアンインストールします。
/L [i|w|e|a|r |u|c|m|p|v|+] *log file*	**/L** オプションを使用して作成すると、ログ・ファイルへのパスが指定されます。以下のフラグは、ログ・ファイルに記録する情報を示しています。 • **i** は、状況メッセージをログに記録します • **w** は、致命的でない警告メッセージをログに記録します • **e** は、すべてのエラー・メッセージをログに記録します • **a** は、アクション・シーケンスの開始をログに記録します • **r** は、アクション固有のレコードをログに記録します • **u** は、ユーザー要求をログに記録します • **c** は、初期ユーザー・インターフェース・パラメーターをログに記録します • **m** は、メモリー不足メッセージをログに記録します • **p** は、端末設定をログに記録します • **v** は、冗長出力設定をログに記録します • **+** は、既存ファイルに付加します • ***** は、すべての情報を (冗長出力設定を除いて) ログに記録できるワイルドカード文字です

表 39. コマンド・ライン・パラメーター (続き)

パラメーター	説明
/q [n|b|r|f]	/q オプションを以下のフラグと併用して、ユーザー・インターフェース・レベルを設定します。 • **q** または qn は、ユーザー・インターフェースを作成しません。 • **qb** は、基本ユーザー・インターフェースを作成します。 下記のユーザー・インターフェース設定により、インストール終了時にモーダル・ダイアログ・ボックスが表示されます。 • **qr** は、縮小ユーザー・インターフェースを表示します。 • **qf** は、完全なユーザー・インターフェースを表示します。 • **qn+** は、ユーザー・インターフェースを表示しません。 • **qb+** は、基本ユーザー・インターフェースを表示します。
/? または /h	いずれかのコマンドにより、Windows インストーラーの著作権情報が表示されます。
TRANSFORMS	**TRANSFORMS** コマンド・ライン・パラメーターを使用して、基本パッケージに適用する変換を指定します。 `msiexec /i "C:¥`*`WindowsFolder`*`¥` `Profiles¥`*`UserName`*`¥Personal ¥MySetups¥` `Your Project Name¥Trial Version¥` `My Release-1 ¥DiskImages¥Disk1¥` `ProductName.msi" TRANSFORMS="New Transform 1.mst"` 複数の変換をセミコロンで分離できます。Windows インストーラー・サービスが誤って解釈しないように、変換の名前にセミコロンを使用しないでください。

表 39. コマンド・ライン・パラメーター (続き)

パラメーター	説明
Properties	すべての共通プロパティはコマンド・ラインで設定または変更できます。共通プロパティは専用プロパティと区別され、すべて大文字です。たとえば、*COMPANYNAME* は共通プロパティです。 コマンド・ラインからプロパティを設定するには、次の構文を使用します。 `PROPERTY=VALUE` *COMPANYNAME* の値を変更するには、次のように入力します。 `msiexec /i "C:¥`*`WindowsFolder`*`¥` `Profiles¥`*`UserName`*`¥Personal` `¥` `MySetups¥`*`Your Project Name`*`¥` `Trial Version¥My Release-1` `¥` `DiskImages¥Disk1¥`*`ProductName.msi`*`"` *`COMPANYNAME`*`="InstallShield"`

付録 B. Rescue and Recovery のカスタマイズ

Rescue and Recovery のカスタマイズは、現在ではレジストリーを介して行われます。インストール時に rnrdeploy.xml ファイルが使用されて、Rescue and Recovery の設定がカスタマイズされます。この XML ファイルは、Active Directory のグループ・ポリシーの ADM ファイルに似ています。 XML ファイルのレジストリー設定値を表示するには、Lenovo Web サイト http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN (英語のサイトです) にある XML ファイルをダウンロードします。

Rescue and Recovery の以前のバージョンは tvt.txt ファイルを使用してカスタマイズされていました。 tvt.txt ファイルには、Rescue and Recovery の設定が含まれていました。Lenovo は、Rescue and Recovery のカスタマイズ・プロセスを再設計して、現在ではレジストリーを使用しています。Rescue and Recovery を以前のバージョンの上にインストールする場合、tvt.txt ファイルの設定値はレジストリーに移行されます。

バックアップおよび関連タスクのスケジューリング

スケジューラーは Rescue and Recovery 固有に設計されていませんが、構成はレジストリーに保管されます。Rescue and Recovery がインストールされると、スケジューラーは適切な設定値で取り込まれます。

以下に、スケジューラーの構造の説明を示します。
- 場所: インストール・フォルダー。
- スケジュールを設定された各タスクの項目。
- 実行スクリプト。
- 進行状況の通知に使用される名前付きパイプ。これはオプションの設定です。
- スケジュール情報、つまり毎月、毎週、毎日、平日、または週末 (複数のスケジュール。たとえば、火曜日と金曜日は 2 つのスケジュールを作成することによりサポートされます。)
- タスクに受け渡されるパラメーター。

Rescue and Recovery の場合、スケジュールに沿って増分バックアップを行い、バックアップの前後にコールバックを送ってください。

バックアップ用ネットワーク・ドライブの割り当て

ネットワーク・ドライブの割り当て機能は、HKLM¥Software¥Lenovo¥MND にあるレジストリー設定値に依存します。

汎用命名規則 (UNC) 項目には、接続先の PC 名および共有が含まれます。

NetPath 項目は、mapdrv.exe からの出力される値です。これには、接続の作成時に使用された実際の名前が含まれます。

User および Pwd 項目は、ユーザー名およびパスワードの項目です。これらは暗号化されています。

以下に、ネットワーク・ドライブの割り当てを行うための項目の例を示します。

```
UNC=¥¥server¥share

NetPath=¥¥9.88.77.66¥share

User=11622606415119207723014918505422010521006401209203708202015...

Pwd=11622606415100000000001491850542201052100640120920370820201 5...
```

デプロイメントの際、このファイルを同じユーザー名およびパスワードを使用する複数の PC で使用するようにコピーすることができます。UNC 項目は、Rescue and Recovery により rnrdeploy.xml ファイルの値に従って上書きされます。

ネットワーク・バックアップ用のユーザー・アカウントのセットアップ

ネットワーク共有フォルダー上に RRBACKUPS フォルダーが作成されるとき、Rescue and Recovery のサービスにより、このフォルダーは読み取り専用フォルダーとして作成され、フォルダーを作成したアカウントのみ がフォルダーに対して完全な制御を持つようにアクセス権が割り当てられます。

マージ操作を完了するには、バックアップを作成しているユーザー・アカウントの変更許可が必要です。フォルダーを最初に作成したアカウント以外のアカウント (たとえば、管理者) でログインすると、マージ・コマンドは失敗してしまいます。これを回避するには、
1. 制限ユーザーでバックアップを取る。
2. ネットワークへのバックアップと同時にローカルへのバックアップも取る。
のどちらかを行うようにしてください。

付録 C. コマンド・ライン・ツール

企業の IT 管理者はコマンドライン・インターフェースを使用して、ローカルまたはリモートから ThinkVantage テクノロジーの機能を実装することもできます。設定情報は、リモートのテキスト・ファイル設定を介して保守することができます。

Antidote Delivery Manager

このセクションでは、Antidote Delivery Manager のコマンド・ラインの手順について説明します。

Mailman

Antidote Delivery Manager は、コマンド C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM¥mailman.exe を使用します。この手順は、実行するタスクの Antidote リポジトリーを確認します。コマンド・ライン引数はありません。

Antidote ウィザード

Antidote ウィザードの実行可能プログラム (AWizard.exe) は、管理者がインストールした場所に配置されます。コマンド・ライン引数はありません。

パスワードの設定

SETPASSWORD コマンドは、PrivateDisk ボリュームにユーザー・パスワードを設定します。パスワードについては、 40 ページの『パスワード』を参照してください。

Client Security Solution

Client Security Solution には次のコマンド・ライン・ツールがあります。

SafeGuard PrivateDisk

コマンド・ライン・インターフェースは C:¥Program Files¥Lenovo¥SafeGuard PrivateDisk¥ フォルダーにあります。構文は次のとおりです。

```
PDCMD
 [ADDCERT volumename /pw adminpassword /sn certSN [/acc access]]  |
 [LIST]  |
 [MOUNT volumename [/pw userpassword [/pt authmode]] [/ro]]  |
 [NEW volumename [/sz size] [/dl driveletter] [/fs filesystem]
   [/pw adminpassword] [/pwu userpassword]]  |
 [UNMOUNT volumename /f]  |
 [UNMOUNTALL [/f]]  |
 [SETPASSWORD volumename /pw adminpassword /pwu userpassword [/ro]]
```

パラメーターは表 40 に表示されます。

表 40.

パラメーター	結果
ADDCDERT	PrivateDisk ボリュームに証明書を追加します。
LIST	このユーザーの PrivateDisk ボリュームをリストします。
MOUNT	特定の PrivateDisk ボリュームをマウントします。
NEW	新規 PrivateDisk ボリュームを作成します。
UNMOUNT	特定の PrivateDisk ボリュームを取り外します。
UNMOUNTALL	すべての PrivateDisk ボリュームを取り外します。
SETPASSWORD	PrivateDisk ボリュームにユーザー・パスワードを設定します。
VOLUMENAME	PrivateDisk ファイルを含むファイルの名前を指定します。
PW	パスワードを指定します。
SN	証明書のシリアル番号を指定します。
ACC	追加する証明書のアクセス・タイプを設定します。有効な値は次のとおりです。 • **adm** 管理者のアクセス • **uro** ユーザーの読み取り専用アクセス • **usr** ユーザーの書き込みアクセス (デフォルト)
PT	認証方式を設定します。有効な値は次のとおりです。 • **0** 管理者のアクセス (デフォルト) • **1** ユーザー・パスワード • **2** 証明書に基づくログインの PIN
RO	ファイルが読み取り専用であるかどうかを決定します。
SZ	ファイル・サイズ (KB) を指定します。

表 40. (続き)

パラメーター	結果
DL	PrivateDisk ボリュームのドライブ名 (デフォルト = 使用可能な次のドライブ名) を指定します。
FS	ファイル・システム値を指定します。デフォルト値は次のとおりです。 • FAT (デフォルト) • NTFS
PWU	ユーザー・パスワードを指定します。
F	操作を強制します。

Security Advisor

Client Security Solution から Security Advisor を実行するには、「**スタート**」→「**プログラム**」→「**すべてのプログラム**」→「**ThinkVantage**」→「**Client Security Solution**」とクリックします。「**拡張**」をクリックして、「**セキュリティー設定の監査**」を選択します。これにより、C:¥Program Files¥Lenovo¥Common Files¥WST¥wst.exe がデフォルトでインストールされます。

パラメーターは次のとおりです。

表 41.

パラメーター	説明
HardwarePasswords	ハードウェア・パスワードの値を設定します。1 はこのセクションを表示し、0 は隠します。デフォルトは、1 です。
PowerOnPassword	PowerOn パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
HardDrivePassword	ハードディスクのパスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
AdministratorPassword	管理者パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
WindowsUsersPasswords	Windows ユーザー・パスワードの値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
Password	ユーザー・パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
PasswordAge	この PC 上での、Windows のパスワードの使用日数の値を設定するか、設定にフラグを立てる値を設定します。
PasswordNeverExpires	Windows のパスワードが期限切れにならない値を設定するか、設定にフラグを立てる値を設定します。

表 41. (続き)

パラメーター	説明
WindowsPasswordPolicy	Windows パスワード・ポリシーの値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
MinimumPasswordLength	この PC 上でのパスワードの長さの値を設定するか、設定にフラグを立てる値を設定します。
MaximumPasswordAge	この PC 上でのパスワードの使用日数の値を設定するか、設定にフラグを立てる値を設定します。
ScreenSaver	スクリーン・セーバーの値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
ScreenSaverPasswordSet	スクリーン・セーバーにパスワードを要求する値を設定するか、設定にフラグを立てる値を設定します。
ScreenSaverTimeout	この PC 上でのスクリーン・セーバーのタイムアウトの値を設定するか、設定にフラグを立てる値を設定します。
FileSharing	ファイル共有の値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
AuthorizedAccessOnly	ファイル共有のための許可されたアクセスを設定する値を設定するか、設定にフラグを立てる値を設定します。
ClientSecurity	Client Security の値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
EmbeddedSecurityChip	セキュリティー・チップを使用可能にする値を設定するか、設定にフラグを立てる値を設定します。
ClientSecuritySolution	この PC 上で使用する Client Security Solution のバージョンの値を設定するか、設定にフラグを立てる値を設定します。

Client Security Solution セットアップ・ウィザード

Client Security Solution セットアップ・ウィザードはハードウェアの所有権を取得し、ソフトウェアを構成し、ユーザーを登録するために使用します。XML ファイルを介してデプロイメント・スクリプトを生成する際にも使用します。次のコマンドを実行すると、ウィザードのさまざまな機能が表示されます。

```
C:¥Program Files¥Lenovo¥Client Security Solution¥css_wizard.exe /?
```

次の表に、Client Security Solution セットアップ・ウィザードのコマンドを示します。

表 42.

パラメーター	結果
/h または /?	ヘルプ・メッセージ・ボックスを表示します
/name:*FILENAME*	生成されたデプロイメント・ファイルの完全修飾パスおよびファイル名の前に付けます。このファイルには拡張子 .xml が付きます。
/encrypt	AES 暗号化を使用してスクリプト・ファイルを暗号化します。暗号化される場合、そのファイル名には .enc が付加されます。 /pass コマンドを使用しない場合は、静的パスフレーズを使用して、ファイルを隠します。
/pass:	暗号化されたデプロイメント・ファイルを保護するために、パスフレーズの前に付けます。
/novalidate	ウィザードのパスワードとパスフレーズのチェック機能を使用不可にして、すでに構成済みの PC 上でスクリプト・ファイルを作成できるようにします。たとえば、現行 PC の管理者パスワードは、社内で要求される管理者パスワードではないことがあります。/novalidate コマンドを使用するとユーザーは xml ファイル作成中に css_wizard GUI に別の管理者パスワードを入力できます。

例:

```
css_wizard.exe /encrypt /pass:my secret /name:C:¥DeployScript /novalidate
```

デプロイメント・ファイルの暗号化または暗号化解除ツール

このツールは Client Security XML デプロイメント・ファイルの暗号化または暗号化解除に使用します。次のコマンドを実行すると、ツールのさまざまな機能が表示されます。

```
C:¥Program Files¥Lenovo¥Client Security Solution¥xml_crypt_tool.exe. /?
```

パラメーターは表 43 に表示されます。

表 43.

パラメーター	結果
/h または /?	ヘルプ・メッセージを表示します
FILENAME	.xml または .enc の拡張子を持つパス名およびファイル名を表示します。
encrypt または decrypt	.xml ファイルには /encrypt、.enc ファイルには /decrypt を選択します。

表 43. (続き)

パラメーター	結果
PASSPHRASE	ファイルを保護するためにパスフレーズを使用する場合に必要なオプション・パラメーターを表示します。

例:

```
xml_crypt_tool.exe "C:¥DeployScript.xml" /encrypt "my secret"
```

および

```
xml_crypt_tool.exe "C:¥DeployScript.xml.enc" /decrypt "my secret"
```

デプロイメント・ファイル処理ツール

ツール vmserver.exe は Client Security Solution XML デプロイメント・スクリプトを処理します。次のコマンドを実行すると、ウィザードのさまざまな機能が表示されます。

```
C:¥Program Files¥Lenovo¥Client Security Solution¥vmserver.exe /?
```

次の表に、ファイルを処理するためのパラメーターを示します。

表 44.

パラメーター	結果
FILENAME	FILENAME パラメーターにはファイル拡張子 XML または ENC がなければなりません。
PASSPHRASE	PASSPHRASE パラメーターは、拡張子 ENC を持つファイルの暗号化解除に使用します。

例:

```
Vmserver.exe  C:¥DeployScript.xml.enc "my secret"
```

TPMENABLE.EXE

tpmenable.exe ファイルはセキュリティー・チップをオンにしたりオフにするために使用します。

表 45.

パラメーター	説明
/enable または /disable	セキュリティー・チップをオンにしたりオフにしたりします。
/quiet	BIOS パスワードまたはエラーのプロンプトを隠します。
sp:*password*	BIOS 管理者/スーパーバイザーのパスワードです。パスワードの前後に引用符を使用してはいけません。

例:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

Active Directory のサポート

Active Directory はディレクトリー・サービスです。ディレクトリーは、ユーザーおよびリソースに関する情報が保管されている場所です。ディレクトリー・サービスによりアクセスが許可されるため、これらのリソースを操作することができます。

Active Directory が提供する機構により、管理者は PC、グループ、ユーザー、ドメイン、セキュリティー・ポリシー、およびすべてのタイプのユーザー定義オブジェクトを管理する機能を得られます。Active Directory がこの機能を付与するために使用する機構のことを、グループ・ポリシーといいます。管理者は、グループ・ポリシーを使用して、PC やユーザーに適用できる設定をドメイン中に定義します。

現在 ThinkVantage テクノロジー製品が使用している、プログラム設定の制御に使用する設定値を収集する方式には、特定のアプリケーション定義レジストリー項目からの読み取りなど、さまざまな方式があります。

以下に、Active Directory が管理できる ThinkVantage テクノロジー製品の設定の例を示します。

- Rescue and Recovery
  - バックアップの場所を設定します。
  - バックアップの日付と時間を設定します。
- Client Security Solution
  - セキュリティー・ポリシーを設定します。
  - カスタム・セキュリティー・ポリシーを設定します (Windows パスワードまたは Client Security Solution パスフレーズを使用するかどうか、など)。

管理用 (ADM) テンプレート・ファイル

ADM (管理用) テンプレート・ファイルは、クライアント PC 上のアプリケーションで使用されるポリシー設定を定義します。ポリシーとは、アプリケーションの動作を管理する特定の設定のことです。ポリシー設定は、ユーザーがアプリケーションを使用して特定の設定値を設定できるかどうかも定義します。

サーバー上の管理者が定義する設定は、ポリシーとして定義されます。クライアント PC 上のユーザーが定義する、アプリケーションに関する設定は、プリファレンスとして定義されます。Microsoft 社による定義のとおりに、ポリシー設定はプリファレンスより優先します。

例えば、ユーザーは自分のデスクトップ上に背景イメージを表示することができます。これは、ユーザーのプリファレンス設定です。管理者は、ユーザーが特定の背景イメージを使用しなければならないことを決定する設定をサーバー上で定義できます。管理者のポリシー設定は、ユーザーによるプリファレンス設定をオーバーライドします。

ThinkVantage テクノロジー製品が設定を検査する際に、次の順序で設定を検索します。

- コンピューター・ポリシー
- ユーザー・ポリシー
- デフォルトのユーザー・ポリシー

- PC プリファレンス
- ユーザー・プリファレンス
- デフォルトのユーザー・プリファレンス

前述のように、コンピューター・ポリシーとユーザー・ポリシーは、管理者によって定義されます。XML 構成ファイルか Active Directory のグループ・ポリシーを使用してこれらの設定値を初期化できます。PC プリファレンスとユーザー・プリファレンスは、クライアント PC 上のユーザーによって、アプリケーション・インターフェース内のオプションを使用して設定されます。デフォルトのユーザー・プリファレンスは、XML 構成スクリプトによって初期化されます。ユーザーは値を直接には変更しません。ユーザーがこれらの設定値に変更を加えるには、ユーザー・プリファレンスを更新します。

Active Directory を使用していないお客様は、クライアント・システムにデプロイされるポリシー設定のデフォルト・セットを作成することができます。管理者は、XML 構成スクリプトを変更して、製品のインストール時にそれらが処理されるように指定することができます。

管理可能設定の定義

この例では、次の階層を使用して、グループ・ポリシー・エディター内に設定を表示します。

```
Computer Configuration>Administrative Templates>ThinkVantage Technologies>
Client Security Solution>Authentication Policies>Max Retries>
Password number of retries
```

ADM ファイルは、レジストリー内の、設定が反映される場所を示します。これらの設定は、レジストリー内の次の場所になければなりません。

```
Computer policies:
HKLM¥Software¥Policies¥Lenovo¥Rescue and Recovery¥
HKLM¥Software¥Policies¥Lenovo¥Client Security Solution¥

User policies:
HKCU¥Software¥Policies¥Lenovo¥Rescue and Recovery¥
HKCU¥Software¥Policies¥Lenovo¥Client Security Solution¥

Default user policies:
HKLM¥Software¥Policies¥Lenovo¥Rescue and Recovery¥User defaults
HKLM¥Software¥Policies¥Lenovo¥Client Security Solution¥User defaults

Computer preferences:
HKLM¥Software¥Lenovo¥Rescue and Recovery¥
HKLM¥Software¥Lenovo¥Client Security Solution¥

User preferences:
HKCU¥Software¥Lenovo¥Rescue and Recovery¥
HKCU¥Software¥Lenovo¥Client Security Solution¥

Default user preferences:
HKLM¥Software¥Lenovo¥Rescue and Recovery¥User defaults
HKLM¥Software¥Lenovo¥Client Security Solution¥User defaults
```

グループ・ポリシーの設定

このセクションの表には、Rescue and Recovery および Client Security Solution の PC 構成およびユーザー構成のポリシー設定が記載されています。

Rescue and Recovery

このセクションの表には、Rescue and Recovery のポリシー設定が記載されています。

ユーザー構成: 次の表に、「ユーザー構成」の「設定」タブのポリシーを示します。

表 46. ユーザー構成>Rescue and Recovery>設定

ポリシー	説明
Analyze FileSize Threshold	分析機能がファイルを表示するかどうかを判別するために使用するしきい値を表示します。値: 0 から 10,000 MB。デフォルト: 20 MB。
Sort Filter Files	「バックアップから除外するファイル」、「追加」、および「SIS」ページで表示するファイル・ソートのタイプを表示します。値: 1 から 4 (名前の昇順、名前の降順、サイズの昇順、サイズの降順)。デフォルト: 0 (ソートなし)。

ユーザー・インターフェース: 次の表に、「ユーザー・インターフェース」のポリシー設定を示します。

表 47. ユーザー構成>Rescue and Recovery>ユーザー・インターフェース

ポリシー	設定	説明
メニュー	「バックアップ」メニュー	「バックアップ」メニューを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー	「復元」メニュー	メイン・ユーザー・インターフェースの「復元」メニューを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー	「拡張」メニュー	メイン・ユーザー・インターフェースの「拡張」メニューを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー	「ヘルプ」メニュー	メイン・ユーザー・インターフェースの「ヘルプ」メニューを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	ハードディスクのバックアップ	メイン・ユーザー・インターフェースの「ハードディスクのバックアップ」メニュー項目およびボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	スケジュールと項目の設定	メイン・ユーザー・インターフェースの「スケジュールと項目の設定」メニュー項目およびボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	バックアップ保存容量の最適化	メイン・ユーザー・インターフェースの「バックアップ保存容量の最適化」メニュー項目およびボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。

表 47. ユーザー構成>Rescue and Recovery>ユーザー・インターフェース (続き)

ポリシー	設定	説明
メニュー項目	すべてのバックアップの表示	メイン・ユーザー・インターフェースの「すべてのバックアップの表示」メニュー項目およびボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	バックアップからシステムを復元する	メイン・ユーザー・インターフェースの「バックアップからシステムを復元する」メニュー項目およびボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	個別のファイルを復元する	メイン・ユーザー・インターフェースの「個別のファイルを復元する」メニュー項目およびボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	ハードディスクからバックアップをコピー	メイン・ユーザー・インターフェースの「ハードディスクからバックアップをコピー」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	バックアップの削除	メイン・ユーザー・インターフェースの「バックアップの削除」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	バックアップから除外するファイル	メイン・ユーザー・インターフェースの「バックアップから除外するファイル」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	追加	メイン・ユーザー・インターフェースの「追加」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	Single Storage のファイルの指定	メイン・ユーザー・インターフェースの「Single Storage のファイルの指定」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	マイグレーション・ファイルの作成	メイン・ユーザー・インターフェースの「マイグレーション・ファイルの作成」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	Sysprep バックアップ	メイン・ユーザー・インターフェースの「Sysprep バックアップ」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 非表示。
メニュー項目	ヘルプ・トピック	メイン・ユーザー・インターフェースの「ヘルプ・トピック」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	コンテキスト・ヘルプ	メイン・ユーザー・インターフェースの「コンテキスト・ヘルプ」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	Active Update	メイン・ユーザー・インターフェースの「Active Update」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。

表 47. ユーザー構成>Rescue and Recovery>ユーザー・インターフェース (続き)

ポリシー	設定	説明
メニュー項目	ユーザー・ガイド	メイン・ユーザー・インターフェースの「ユーザー・ガイド」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
メニュー項目	Rescue and Recovery について	メイン・ユーザー・インターフェースの「Rescue and Recovery について」メニュー項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
バックアップ	バックアップ保存先	データをバックアップするためのラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
バックアップ	バックアップを CD/DVD に作成	光ディスクにバックアップを作成するためのラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
バックアップ	最大増分数の超過 (Max Incrementals Exceeded)	「最大増分数の超過 (Max Incrementals Exceeded)」ダイアログを表示するか、非表示にします。デフォルト: 非表示。
復元	ハードディスク全体を復元	「ハードディスク全体を復元」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。
復元	システムを活性化する	復元オプションの「システムを活性化する」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
復元	OS およびアプリケーションのみを復元	復元オプションの「OS およびアプリケーションのみを復元」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
復元	SFR NTFS を Fat32 に復元 (SFR Restore NTFS To Fat32)	NTFS からファイルを復元する際に Fat32 区画を表示するか、非表示にします。デフォルト: 表示。
復元	レスキューするファイルの「検索」	「レスキューするファイルの「検索」」ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
復元	パスワードの保存 (Password Persist)	「パスワードの保存 (Password Persist)」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
復元	基本バックアップ	ユーザー・インターフェースを介して復元する基本バックアップを表示するか、非表示にします。デフォルト: 表示。
復元	管理者バックアップ (Admin Backups)	ユーザー・インターフェースを介して復元する「管理者バックアップ (Admin Backups)」を表示するか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	バックアップ保存先「プライマリー」	「スケジュールと項目の設定」ダイアログの「バックアップ保存先「プライマリー」」を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	バックアップ保存先「セカンダリー」	「スケジュールと項目の設定」ダイアログの「バックアップ保存先「セカンダリー」」を表示するか、ぼかすか、非表示にします。デフォルト: 表示。

表 47. ユーザー構成>Rescue and Recovery>ユーザー・インターフェース (続き)

ポリシー	設定	説明
スケジュールと項目の設定	バックアップのスケジュール	「スケジュールと項目の設定」ダイアログの「バックアップのスケジュール」を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	頻度	「スケジュールと項目の設定」ダイアログの「頻度」を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	日付	「スケジュールと項目の設定」ダイアログの「日付」を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	「中断」チェック (Suspend Check)	「スケジュールと項目の設定」ダイアログの「中断 (Suspend)」チェック・ボックスを表示するか、ぼかすか、非表示にします。デフォルト: 非表示。
スケジュールと項目の設定	追加する区画	「スケジュールと項目の設定」ダイアログの「追加する区画」チェック・ボックスを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	バックアップが次の容量を超えたら警告する	「スケジュールと項目の設定」ダイアログの「バックアップが次の容量を超えたら警告する」項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	パスワードでバックアップを保護する	「スケジュールと項目の設定」ダイアログの「パスワードでバックアップを保護する」項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	CSS 暗号化 (CSS Encrypt)	「スケジュールと項目の設定」ダイアログの「CSS 暗号化 (CSS Encrypt)」項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
スケジュールと項目の設定	ハードディスクのロック	「スケジュールと項目の設定」ダイアログの「ハードディスクのロック」項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
ハードディスクからバックアップをコピー	CD/DVD	「CD/DVD」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
ハードディスクからバックアップをコピー	USB	「USB」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
ハードディスクからバックアップをコピー	セカンド・ハードディスク	「セカンド・ハードディスク」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
ハードディスクからバックアップをコピー	ネットワーク	「ネットワーク」ラジオ・ボタンを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
バックアップの削除	基本バックアップ	削除ページの基本バックアップを表示するか、非表示にします。デフォルト: 表示。
マイグレーション・ファイルの作成	『ファイルの選択』ボタンをクリックしてこのデバイスからファイルを削除する	「マイグレーション・ファイルの作成」ページの「『ファイルの選択』ボタンをクリックしてこのデバイスからファイルを削除する項目」を表示するか、ぼかすか、非表示にします。デフォルト: 表示。

表 47. ユーザー構成>Rescue and Recovery>ユーザー・インターフェース (続き)

ポリシー	設定	説明
マイグレーション・ファイルの作成	マイグレーションの「パスワード」	「マイグレーション・ファイルの作成」ページの「マイグレーションの「パスワード」」項目を表示するか、ぼかすか、非表示にします。デフォルト: 表示。
ユーザー・インターフェース		メイン・ユーザー・インターフェースを使用可能または使用不可にします。デフォルト: 使用可能。
「復元」インターフェース		「復元」インターフェースを使用可能または使用不可にします。デフォルト: 使用可能。

注: Active Directory テンプレートを使用して画面全体を削除しようとする場合は、画面の各項目で「非表示」を使用するのではなく、メニュー項目を使用不可にしてください。

PC 構成:

次の表に、Rescue and Recovery の「PC 構成」の「設定」タブの下にあるポリシー設定を示します。

表 48. PC 構成>Rescue and Recovery>設定

ポリシー	設定	サブ設定	説明
バックアップ	PreBackup	Pre	バックアップの前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters	バックアップの前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PreBackup	PreShow	バックアップの前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
バックアップ	PreBackup	Pre0	基本バックアップの前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters0	基本バックアップの前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	PreBackup	PreShow0	基本バックアップの前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
バックアップ	PreBackup	Pre1	増分バックアップ番号 1 の前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters1	増分バックアップ番号 1 の前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PreBackup	PreShow1	増分バックアップ番号 1 の前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
バックアップ	PreBackup	Pre2	増分バックアップ番号 2 の前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters2	増分バックアップ番号 2 の前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PreBackup	PreShow2	増分バックアップ番号 2 の前に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。
バックアップ	PreBackup	Pre3	増分バックアップ番号 3 の前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters3	増分バックアップ番号 3 の前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PreBackup	PreShow3	増分バックアップ番号 3 の前に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	PreBackup	Pre4	増分バックアップ番号 4 の前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters4	増分バックアップ番号 4 の前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PreBackup	PreShow4	増分バックアップ番号 4 の前に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。
バックアップ	PreBackup	Pre5	増分バックアップ番号 5 の前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PreBackup	PreParameters5	増分バックアップ番号 5 の前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PreBackup	PreShow5	増分バックアップ番号 5 の前に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。
バックアップ	PostBackup	Post	バックアップが終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters	バックアップの終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow	バックアップの後に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	PostBackup	Post0	基本バックアップが終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters0	基本バックアップの終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow0	基本バックアップの後に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
バックアップ	PostBackup	Post1	増分バックアップ番号 1 が終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters1	増分バックアップ番号 1 の終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow1	増分バックアップ番号 1 の後に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。
バックアップ	PostBackup	Post2	増分バックアップ番号 2 が終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters2	増分バックアップ番号 2 の終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow2	増分バックアップ番号 2 の後に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	PostBackup	Post3	増分バックアップ番号 3 が終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters3	増分バックアップ番号 3 の終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow3	増分バックアップ番号 3 の後に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。
バックアップ	PostBackup	Post4	増分バックアップ番号 4 が終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters4	増分バックアップ番号 4 の終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow4	増分バックアップ番号 4 の後に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。
バックアップ	PostBackup	Post5	増分バックアップ番号 5 が終了した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
バックアップ	PostBackup	PostParameters5	増分バックアップ番号 5 の終了後に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
バックアップ	PostBackup	PostShow5	増分バックアップ番号 5 の後に実行されるコマンドを表示するか、非表示にします。デフォルト:表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	Backup Local		バックアップ用に選択された宛先として「ローカルのバックアップ (Backup Local)」を使用可能または使用不可にします。デフォルト: 使用可能。
バックアップ	Backup Second		バックアップ用に選択された宛先として「2 次のバックアップ (Backup Second)」を使用可能または使用不可にします。デフォルト: 使用不可。
バックアップ	Backup USB		バックアップ用に選択された宛先として「USB のバックアップ (Backup USB)」を使用可能または使用不可にします。デフォルト: 使用不可。
バックアップ	Backup Network		バックアップ用に選択された宛先として「ネットワークのバックアップ (Backup Network)」を使用可能または使用不可にします。デフォルト: 使用不可。
バックアップ	Local Partition Number		ローカル・ドライブ上のバックアップの区画番号を設定します。有効な値: 1 から 100。デフォルト: 1。
バックアップ	USB Partition Number		USB ドライブ上のバックアップの区画番号を設定します。有効な値: 1 から 100。デフォルト: 1。
バックアップ	Second HDD Partition Number		セカンド・ハードディスク上のバックアップの区画番号を設定します。有効な値: 1 から 100。デフォルト: 1。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	Backup Partitions		バックアップする区画を選択します。この DWORD は、バックアップに含める論理ドライブ名のビットマップです。たとえば、ドライブ c: および e: のみをバックアップする場合、この値は 0x00000014 です。注: 入力する前に 16 進数を 10 進数に変換してください。デフォルト: 0xFFFFFFFF。ゼロを入力すると、デフォルトと似た意味になります。使用可能な区画をすべて見つけて、バックアップしてください。
バックアップ	Max Backup Size		最大バックアップ・サイズ (GB)。有効な値は 1 から 1000 です。デフォルト: 使用可能な空き領域。
バックアップ	Max Number Incrementals		許容される増分バックアップの最大数。有効な値: 2 から 31。デフォルト: 5。**注:** バックアップ番号 5 を完了してから、バックアップ番号 6 に進むと、次のメッセージが表示されます。*設定された次の制限容量に達しました: 増分バックアップ 5 つ。(You have reached your defined limit of 5 incremental backups.) 許可される増分バックアップの最大数を増やすことができます。そうでない場合は、最も古い増分バックアップが削除されます。(You may increase the maximum number of incremental backups allowed or the oldest incremental backup will be deleted.)*このメッセージは、最も古い増分バックアップを削除せずに、次の増分バックアップにマージできることを通知しています。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	Encrypt With CSS		バックアップ・オプションとして「Client Security Solution を使用する暗号化 (Encrypt With Client Security Solution)」を使用可能または使用不可にします。このオプションは、ハードウェアまたは静的鍵の暗号化を許可します。デフォルト: 使用不可。
バックアップ	Resume After Power Loss		バックアップ・オプションとして「電力損失の後に再開する (Resume After Power Loss)」を使用可能または使用不可にします。デフォルト: 使用可能。
バックアップ	Capture Migration Info		バックアップ・オプションとして「マイグレーション情報の取り込み (Capture Migration Info)」を使用可能または使用不可にします。使用可能にすると、バックアップごとに、必要に応じて System Migration Assistant が現行システム設定値を別の PC に転送することを許可するデータが収集されます。デフォルト: 使用可能。
バックアップ	Backup SP Second		オプションとして「SP の 2 次へのバックアップ (Backup SP Second)」を使用可能または使用不可にします。使用可能にすると、システムのサービス区画を 2 番目のシステム・ドライブにバックアップすることができます。デフォルト: 使用不可。
バックアップ	Backup SP USB		オプションとして「SP の USB へのバックアップ (Backup SP USB)」を使用可能または使用不可にします。使用可能にすると、システムのサービス区画を USB ドライブにバックアップすることができます。デフォルト: 使用不可。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	Backup SP Network		オプションとして「SP のネットワークへのバックアップ (Backup SP Network)」を使用可能または使用不可にします。使用可能にすると、システムのサービス区画をネットワークにバックアップすることができます。デフォルト: 使用不可。
バックアップ	CPU Priority		バックアップの CPU 優先度。値: 1 から 5 (1 = 最低の優先度、5 = 最高の優先度)。デフォルト: 3。
バックアップ	Yield		「譲歩 (Yield)」は、バックアップ中のディスク書き込みの間に挿入する遅延の時間を示します。これにより、システム・バックアップがすべてのディスク入出力処理能力を占有することが許可されます。値: 0 から 8 (0 = オフ、8 = 最小ディスク・アクティビティー) デフォルト: 0。
バックアップ	Boot Disc		CD/DVD にバックアップする場合、またはこれらのメディアにアーカイブを作成する場合に、「起動ディスク (Boot Disc)」の作成を使用可能または使用不可にします。デフォルト: 使用可能。
バックアップ	VerifyDisc		CD/DVD にバックアップする場合、またはこれらのメディアにアーカイブを作成する場合に、「ディスクの検査 (Verify Disc)」を使用可能または使用不可にします。デフォルト: 使用可能。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
バックアップ	Battery Percent Required		スケジュールされたバックアップを開始する前の「必要なバッテリーのパーセント (Battery Percent Required)」。このポリシーにより、バックアップを完了するために十分なバッテリー電源が残っていることが保証されます。値: 0 から 100。デフォルト: 0。
バックアップ	Skip Locked Files		バックアップ時の「ロック・ファイルのスキップ (Skip Locked Files)」を使用可能または使用不可にします。使用可能にすると、ロック・ファイルはバックアップされません。デフォルト: 使用不可。
バックアップ	Min Percent Free Space		宛先ドライブでバックアップに必要な空き領域の最小パーセント。値: 0 から 100。デフォルト: 0。
バックアップ	Protect With UUID		「UUID での保護 (Protect With UUID)」オプションを使用可能または使用不可にします。使用可能にすると、1 台の PC で取られたバックアップを別の PC で復元できなくなります。デフォルト: 使用不可。
バックアップ	Protect With Password		「パスワードでの保護」オプションを使用可能または使用不可にします。使用可能にすると、バックアップはパスワードで保護されます。デフォルト: 使用不可。
復元	PreRestore	PreWinRestore	Windows から復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PreWinRestoreParameters	Windows から復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PreRestore	PreWinRestoreShow	Windows から復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PreWinRestore0	Windows から基本バックアップを復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PreWinRestoreParameters0	Windows から基本バックアップを復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PreWinRestoreShow0	Windows から基本バックアップを復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PreWinRestore1	Windows から増分バックアップ番号 1 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PreWinRestoreParameters1	Windows から増分バックアップ番号 1 を復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PreWinRestoreShow1	Windows から増分バックアップ番号 1 を復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PreWinRestore2	Windows から増分バックアップ番号 2 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PreRestore	PreWinRestoreParameters2	Windows から増分バックアップ番号 2 を復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PreWinRestoreShow2	Windows から増分バックアップ番号 2 を復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PreWinRestore3	Windows から増分バックアップ番号 3 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PreWinRestoreParameters3	Windows から増分バックアップ番号 3 を復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PreWinRestoreShow3	Windows から増分バックアップ番号 3 を復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PreWinRestore4	Windows から増分バックアップ番号 4 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PreWinRestoreParameters4	Windows から増分バックアップ番号 4 を復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PreWinRestoreShow4	Windows から増分バックアップ番号 4 を復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PreRestore	PreWinRestore5	Windows から増分バックアップ番号 5 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PreWinRestoreParameters5	Windows から増分バックアップ番号 5 を復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PreWinRestoreShow5	Windows から増分バックアップ番号 5 を復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PrePDARestore	Rescue and Recovery ワークスペースから復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PrePDARestoreParameters	Rescue and Recovery ワークスペースから復元する前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PrePDARestoreShow	Rescue and Recovery ワークスペースから復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PrePDARestore0	Rescue and Recovery ワークスペースから基本バックアップを復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PreRestore	PrePDARestoreParameters0	Rescue and Recovery ワークスペースから基本バックアップを復元する前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PrePDARestoreShow0	Rescue and Recovery ワークスペースから基本バックアップを復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PrePDARestore1	Rescue and Recovery ワークスペースから増分バックアップ番号 1 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PrePDARestoreParameters1	Rescue and Recovery ワークスペースから増分バックアップ番号 1 を復元する前に実行されるコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PrePDARestoreShow1	Rescue and Recovery ワークスペースから増分バックアップ番号 1 を復元する前に実行されるコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PrePDARestore2	Rescue and Recovery ワークスペースから増分バックアップ番号 2 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PrePDARestoreParameters2	Rescue and Recovery ワークスペースから増分バックアップ番号 2 を復元する前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PreRestore	PrePDARestoreShow2	Rescue and Recovery ワークスペースから増分バックアップ番号 2 を復元する前に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PrePDARestore3	Rescue and Recovery ワークスペースから増分バックアップ番号 3 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PrePDARestoreParameters3	Rescue and Recovery ワークスペースから増分バックアップ番号 3 を復元する前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PrePDARestoreShow3	Rescue and Recovery ワークスペースから増分バックアップ番号 3 を復元する前に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PreRestore	PrePDARestore4	Rescue and Recovery ワークスペースから増分バックアップ番号 4 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PrePDARestoreParameters4	Rescue and Recovery ワークスペースから増分バックアップ番号 4 を復元する前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PrePDARestoreShow4	Rescue and Recovery ワークスペースから増分バックアップ番号 4 を復元する前に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PreRestore	PrePDARestore5	Rescue and Recovery ワークスペースから増分バックアップ番号 5 を復元する前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PreRestore	PrePDARestoreParameters5	Rescue and Recovery ワークスペースから増分バックアップ番号 5 を復元する前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PreRestore	PrePDARestoreShow5	Rescue and Recovery ワークスペースから増分バックアップ番号 5 を復元する前に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore	Windowsから復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostWinRestoreParameters	Windows から復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostWinRestoreShow	Windows から復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore0	Windows から基本バックアップを復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostWinRestoreParameters0	Windows から基本バックアップを復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PostRestore	PostWinRestoreShow0	Windows から基本バックアップを復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore1	Windows から増分バックアップ番号 1 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostWinRestoreParameters1	Windows から増分バックアップ番号 1 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostWinRestoreShow1	Windows から増分バックアップ番号 1 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore2	Windows から増分バックアップ番号 2 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostWinRestoreParameters2	Windows から増分バックアップ番号 2 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostWinRestoreShow2	Windows から増分バックアップ番号 2 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore3	Windows から増分バックアップ番号 3 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PostRestore	PostWinRestoreParameters3	Windows から増分バックアップ番号 3 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostWinRestoreShow3	Windows から増分バックアップ番号 3 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore4	Windows から増分バックアップ番号 4 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostWinRestoreParameters4	Windows から増分バックアップ番号 4 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostWinRestoreShow4	Windows から増分バックアップ番号 4 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostWinRestore5	Windows から増分バックアップ番号 5 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostWinRestoreParameters5	Windows から増分バックアップ番号 5 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostWinRestoreShow5	Windows から増分バックアップ番号 5 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PostRestore	PostPDARestore	Rescue and Recovery ワークスペースから復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostPDARestoreParameters	Rescue and Recovery ワークスペースから復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostPDARestoreShow	Rescue and Recovery ワークスペースから復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostPDARestore0	Rescue and Recovery ワークスペースから基本バックアップを復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostPDARestoreParameters0	Rescue and Recovery ワークスペースから基本バックアップを復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostPDARestoreShow0	Rescue and Recovery ワークスペースから基本バックアップを復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostPDARestore1	Rescue and Recovery ワークスペースから増分バックアップ番号 1 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PostRestore	PostPDARestoreParameters1	Rescue and Recovery ワークスペースから増分バックアップ番号 1 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostPDARestoreShow1	Rescue and Recovery ワークスペースから増分バックアップ番号 1 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostPDARestore2	Rescue and Recovery ワークスペースから増分バックアップ番号 2 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostPDARestoreParameters2	Rescue and Recovery ワークスペースから増分バックアップ番号 2 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostPDARestoreShow2	Rescue and Recovery ワークスペースから増分バックアップ番号 2 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostPDARestore3	Rescue and Recovery ワークスペースから増分バックアップ番号 3 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostPDARestoreParameters3	Rescue and Recovery ワークスペースから増分バックアップ番号 3 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	PostRestore	PostPDARestoreShow3	Rescue and Recovery ワークスペースから増分バックアップ番号 3 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostPDARestore4	Rescue and Recovery ワークスペースから増分バックアップ番号 4 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostPDARestoreParameters4	Rescue and Recovery ワークスペースから増分バックアップ番号 4 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostPDARestoreShow4	Rescue and Recovery ワークスペースから増分バックアップ番号 4 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
復元	PostRestore	PostPDARestore5	Rescue and Recovery ワークスペースから増分バックアップ番号 5 を復元した後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
復元	PostRestore	PostPDARestoreParameters5	Rescue and Recovery ワークスペースから増分バックアップ番号 5 を復元した後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
復元	PostRestore	PostPDARestoreShow5	Rescue and Recovery ワークスペースから増分バックアップ番号 5 を復元した後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
復元	Password Persist		復元ダイアログの「パスワードの保存 (Password Persist)」オプションを表示するか、非表示にします。デフォルト: 表示。
システムを活性化する	PreRejuvenate		活性化の復元の前に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
システムを活性化する	PreRejuvenate Parameters		活性化の復元の前に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
システムを活性化する	PreRejuvenate Show		活性化の復元の前に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
システムを活性化する	PostRejuvenate		活性化の復元の後に実行するコマンド。ファイルへの絶対パスが環境変数の中にない場合は、そのパスが含まれます。デフォルト: なし。
システムを活性化する	PostRejuvenate Parameters		活性化の復元の後に実行するコマンドを受け渡すパラメーター。デフォルト: なし。
システムを活性化する	PostRejuvenate Show		活性化の復元の後に実行するコマンドを表示するか、非表示にします。デフォルト: 表示。
システムを活性化する	PostRejuvenate Reboot		活性化の復元の後にシステムの再起動を使用可能または使用不可にします。デフォルト: 使用可能。
割り当て済みのネットワーク・ドライブ (Mapped Network Drive)	UNC		割り当て済みのネットワーク・ドライブの UNC の場所 (形式 ¥¥server¥share)。デフォルト: なし。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
割り当て済みのネットワーク・ドライブ (Mapped Network Drive)	User		mapdrv.exe /view コマンドを使用して、このフィールド用に暗号化された値を作成します。デフォルト: なし。
ユーザー・メッセージ (User Messages)	Bootable Second		「起動可能な 2 次 (Bootable Second)」メッセージを表示するか、非表示にします。デフォルト: 非表示。
ユーザー・メッセージ (User Messages)	Bootable USB		「起動可能な USB (Bootable USB)」メッセージを表示するか、非表示にします。デフォルト: 表示。
ユーザー・メッセージ (User Messages)	Location Not Found		「場所が見つかりません (Location Not Found)」メッセージを表示するか、非表示にします。デフォルト: 表示。注: 場所が USB ドライブである場合、このメッセージは引き続き表示されます。
ユーザー・メッセージ (User Messages)	Missed Backup		「欠落したバックアップ (Missed Backup)」メッセージを表示するか、非表示にします。デフォルト: 表示。
ユーザー・メッセージ (User Messages)	No Battery		「バッテリーなし (No Battery)」メッセージを表示するか、非表示にします。デフォルト: 表示。
ユーザー・メッセージ (User Messages)	Scheduled Base		「スケジュール済みの基本 (Scheduled Base)」メッセージを表示するか、非表示にします。デフォルト: 表示。
ユーザー・メッセージ (User Messages)	Power Loss Backup		「電力損失バックアップ (Power Loss Backup)」メッセージを表示するか、非表示にします。デフォルト: 表示。
ユーザー・メッセージ (User Messages)	Post Rejuvenate Reboot		「活性化の後の再起動 (Post Rejuvenate Reboot)」メッセージを表示するか、非表示にします。デフォルト: 表示。

表 48. PC 構成>Rescue and Recovery>設定 (続き)

ポリシー	設定	サブ設定	説明
ハードディスクのロック			「ハードディスクのロック」設定を使用可能または使用不可にします。デフォルト: 使用不可。
環境変数の解析 (Parse Environment Variables)			「環境変数の解析 (Parse Environment Variables)」設定を使用可能または使用不可にします。デフォルト: 使用可能。
バックアップの前に PP アーカイブを設定 (Set PP Archive Before Backup)			「バックアップの前に PP アーカイブを設定 (Set PP Archive Before Backup)」設定を使用可能または使用不可にします。デフォルト: 使用可能。
サイレント再試行の最大回数 (Max Silent Retries)			ネットワーク共有への「サイレント再試行 (Silent Retries)」の最大数を設定します。デフォルト: 3。
バックアップから除外するファイル			「バックアップから除外するファイル」設定を使用可能または使用不可にします。デフォルト: 使用可能。
追加			「追加」設定を使用可能または使用不可にします。デフォルト: 使用不可。
SIS			「SIS」設定を使用可能または使用不可にします。デフォルト: 使用不可。
ファイル・サイズしきい値の分析 (Analyze FileSize Threshold)			分析機能がファイルを表示するかどうかを判別するために使用するしきい値。値: 0 から 10,000 MB。デフォルト: 20 MB。
フィルター・ファイルのソート (Sort Filter Files)			「バックアップから除外するファイル」、「追加」、および「SIS」ページで表示するファイル・ソートのタイプ。値: 1 から 4 (名前の昇順、名前の降順、サイズの昇順、サイズの降順)。デフォルト: 0 (ソートなし)。

Client Security Solution

このセクションの表には、Client Security Solution のポリシー設定が記載されています。

再試行の最大回数: 次の表に、「認証ポリシー」の「再試行の最大回数」のポリシー設定を示します。

表 49. PC 構成>ThinkVantage>Client Security Solution>認証ポリシー>再試行の最大回数

ポリシー	有効な設定	説明
パスワードの再試行回数 (Password number of retries)	再試行の最大回数は 20 です。	ユーザーがポリシーをオーバーライドする前に Windows パスワードを使用して認証を試行できる最大回数を制御します。
パスフレーズの再試行回数 (Passphrase number of retries)	再試行の最大回数は 20 です。	ユーザーがポリシーをオーバーライドする前に Client Security パスフレーズを使用して認証を試行できる最大回数を制御します。
指紋の再試行回数 (Fingerprint number of retries)	再試行の最大回数は 20 です。	ユーザーがポリシーをオーバーライドする前に指紋を使用して認証を試行できる最大回数を制御します。

より便利: 次の表に、「認証ポリシー」の「より便利」のポリシー設定を示します。

表 50. PC 構成>ThinkVantage>Client Security Solution>認証ポリシー>より便利

ポリシー	有効な設定	説明
パスワード (Password)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定できます。	パスワードが必要であるかどうかを制御します。
パスフレーズ (Passphrase)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定できます。	パスフレーズが必要であるかどうかを制御します。
指紋 (Fingerprint)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定できます。	指紋が必要であるかどうかを制御します。
オーバーライド (Override)	パスワード、パスフレーズ、または指紋をオーバーライドするように設定します。	通常の認証が失敗した場合の「フォールバック」認証の要件を定義します。

より安全: 次の表に、「認証ポリシー」の「より安全」のポリシー設定を示します。

表 51. PC 構成>ThinkVantage>Client Security Solution>認証ポリシー>より安全

ポリシー	有効な設定	説明
パスワード (Password)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定します。	パスワードが必要であるかどうかを制御します。
パスフレーズ (Passphrase)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定します。	パスフレーズが必要であるかどうかを制御します。

表 51. PC 構成>ThinkVantage>Client Security Solution>認証ポリシー>より安全 (続き)

ポリシー	有効な設定	説明
指紋 (Fingerprint)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定します。	指紋が必要であるかどうかを制御します。
オーバーライド (Override)	パスワード、パスフレーズ、または指紋をオーバーライドするように設定します。	通常の認証が失敗した場合の「フォールバック」認証の要件を定義します。

認証ポリシー: 次のポリシーのリストには、各ポリシーの認証レベルを定義する有効な設定が記載されています。有効な設定は、「より便利」、「より安全」、「カスタム」です。

- Windows へのログオン
- PC のロック解除
- Password Manager を開く
- CSP シグニチャー認証レベル
- CSP 暗号化解除認証レベル
- PKCS#11 シグニチャー認証レベル
- PKCS#11 暗号化解除認証レベル
- PKCS#11 ログオン認証レベル

次の表に、上記の認証レベルに対するカスタム設定を示します。

表 52. PC 構成>ThinkVantage>Client Security Solution>認証ポリシー>カスタム

ポリシー	有効な設定	説明
パスワード (Password)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定します。	パスワードが必要であるかどうかを制御します。
パスフレーズ (Passphrase)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定します。	パスフレーズが必要であるかどうかを制御します。
指紋 (Fingerprint)	頻度を「**毎回**」または「**ログオンの度に 1 回 (Once per logon)**」に設定します。	指紋が必要であるかどうかを制御します。
オーバーライド (Override)	パスワード、パスフレーズ、または指紋をオーバーライドするように設定します。	通常の認証が失敗した場合の「フォールバック」認証の要件を定義します。

Password Manager: 次の表に、Password Manager のポリシー設定を示します。

表 53. PC 構成>ThinkVantage>Client Security Solution>Password Manager

ポリシー設定	説明
Password Manager を無効にする	システム始動時に Password Manager が開始するかどうかを制御します。
Internet Explorer サポートを無効にする	Password Manager が Internet Explorer からパスワードを保管できるかどうかを制御します。
Mozilla サポートを無効にする	Password Manager が Mozilla ベース・ブラウザー (Firefox および Netscape など) からパスワードを保管できるかどうかを制御します。

表 53. PC 構成>ThinkVantage>Client Security Solution>Password Manager (続き)

ポリシー設定	説明
Windows アプリケーションのサポートを無効にする	Password Manager が Windows アプリケーションからパスワードを保管できるかどうかを制御します。
自動フィルを無効にする	Password Manager が Web サイトおよび Windows アプリケーションへのデータの自動フィルを行うかどうかを制御します。
ホット・キーを無効にする	Password Manager が Web サイトおよび Windows アプリケーションにデータを入力するためのホット・キーの使用をサポートするかどうかを制御します。
ドメイン・フィルタリングを使用する	Password Manager がドメインに基づいて Web サイトをフィルタリングするかどうかを制御します。
制限付きドメイン	Password Manager がパスワードの保管を禁止されているドメインを制御します。
制限付き Web サイト	Password Manager がパスワードの保管を禁止されている URL を制御します。
制限付きアプリケーション	Password Manager がパスワードの保管を禁止されている Windows アプリケーションを制御します。
ログインの再呼び出し	ログインの再呼び出しの Ctrl + F2 を制御します。
入力後転送ツール	入力後転送ツールの Ctrl + Shift + H を制御します。
Password Manager を開く	ホット・キーの Ctrl + Shift + B を制御します。

PrivateDisk: 次の表に、PrivateDisk のポリシー設定を示します。

表 54. PC 構成>ThinkVantage>Client Security Solution>PrivateDisk

ポリシー設定	説明
デフォルト・ボリュームを無効にする (Disable default volumes)	オプションでデフォルトを作成するかどうかを制御します。
デフォルトのボリューム・サイズ (Default volume size)	デフォルトの PrivateDisk ボリュームのサイズを定義します。
デフォルト・ボリューム・ストレージのパス (Default volume storage path)	ユーザーのデフォルト PrivateDisk ボリュームを作成する場所を定義します。
デフォルト・ボリュームのドライブ名 (Default volume drive letter)	デフォルト PrivateDisk ボリュームに割り当てられるドライブ名を定義します。
デフォルト・ボリュームのファイル名 (Default volume file name)	デフォルト PrivateDisk ボリュームを保持するために使用されるファイル名を定義します。

ユーザー・インターフェース: 次の表に、「ユーザー・インターフェース」のポリシー設定を示します。

表 55. PC 構成>ThinkVantage>Client Security Solution>ユーザー・インターフェース

ポリシー設定	説明
「指紋認証ユーティリティー」オプション	Client Security Solution アプリケーションの指紋認証ユーティリティー・オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「ファイル暗号化 (File encryption)」オプション	Client Security Solution アプリケーションのファイル暗号化オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「セキュリティー設定の監査」オプション	Client Security Solution アプリケーションのセキュリティー設定の監査オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「ディジタル証明書の転送」オプション	Client Security Solution アプリケーションの「ディジタル証明書の転送」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「エンベデッド・セキュリティー・チップの状態変更」オプション	Client Security Solution アプリケーションのセキュリティー・チップの状態オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「セキュリティー・チップのロック解除」オプション	Client Security Solution アプリケーションの「セキュリティー・チップのロック解除」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「Policy Manager」オプション	Client Security Solution アプリケーションの「Policy Manager」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「構成ウィザード」オプション	Client Security Solution アプリケーションの「構成ウィザード」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「Password Manager」オプション	Client Security Solution アプリケーションの「Password Manager」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「ハードウェア・パスワードのリセット」オプション	Client Security Solution アプリケーションの「ハードウェア・パスワードのリセット」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
「Windows パスワードの復元」オプション	Client Security Solution アプリケーションの「Windows パスワードの復元」オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。

ワークステーション・セキュリティー・ツール: 次の表に、「ワークステーション・セキュリティー・ツール」のポリシー設定を示します。

表 56. PC 構成>ThinkVantage>Client Security Solution>ワークステーション・セキュリティー・ツール

ポリシー	設定	説明
ハードウェア・パスワード	ハードウェア・パスワード	ハードウェア・パスワード情報の表示を有効または無効にします。
ハードウェア・パスワード	パワーオン・パスワード	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
ハードウェア・パスワード	ハードディスク・パスワード	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
ハードウェア・パスワード	管理者パスワード	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
Windows ユーザー・パスワード	Windows ユーザー・パスワード	Windows ユーザー・パスワード情報の表示を有効または無効にします。
Windows ユーザー・パスワード	パスワード	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
Windows ユーザー・パスワード	パスワードの使用日数	パスワードが許可される最大日数。
Windows ユーザー・パスワード	パスワードは期限切れにならない	推奨値を「True」、「False」、または「無視 (Ignore)」に設定することができます。
Windows パスワード・ポリシー	Windows パスワード・ポリシー	Windows パスワード・ポリシー情報の表示を有効または無効にします。
Windows パスワード・ポリシー	パスワードの最小文字数	パスワードの最小文字数を指定するか、この値を「無視」します。
Windows パスワード・ポリシー	パスワードの最大使用日数	パスワードの最大使用日数 (日数) を設定するか、結果でこの値を「無視」します。
スクリーン・セーバー	スクリーン・セーバー	Windows パスワード・ポリシー情報の表示を有効または無効にします。
スクリーン・セーバー	スクリーン・セーバー・パスワードの設定	パスワードの最小文字数を指定するか、この値を「無視」します。
スクリーン・セーバー	スクリーン・セーバー・タイムアウト	パスワードの最大使用日数 (日数) を設定するか、結果でこの値を「無視」します。
ファイル共有	ファイル共有	ファイル共有情報の表示を有効または無効にします。
ファイル共有	許可されるアクセス	推奨値を「True」、「False」、または「無視 (Ignore)」に設定することができます。
Client Security	Client Security	Client Security 情報の表示を有効または無効にします。
Client Security	エンベデッド・セキュリティー・チップ	推奨値を有効または無効として選択するか、この設定を無視することを設定します。
Client Security	Client Security Solution バージョン	Client Security Solution の最小推奨バージョンを設定するか、「無視 (Ignore)」を設定します。

eGatherer

eGatherer コマンドは C:¥Program Files¥Common Files¥Lenovo¥egatherer¥egather2.exe にあります。

egather2.exe は収集した情報を使用して EG2 出力を作成します。ホーム・フォルダーに保管する、ローカル XML 出力ファイルも作成できます。

注: EG2 ファイルは内部フォーマットです。

2 つの XML ファイルが作成されます。1 つはシステム情報用で、もう 1 つはデモグラフィック情報用です。 XML ファイルの名前は、メーカー、モデル・タイプおよびシリアル番号を組み合わせて作成されます。たとえば、Lenovo-2373Q1U-99MA4L7.XML、Lenovo-2373Q1U-99MA4L7.DEMOGRAPHICS.XML のようになります。

スキャナーは、次のコマンド・ライン構文を使用して、コマンド・ラインから実行できます。

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe probename *probename*]

- **-help**

  短いヘルプ・メッセージを表示します。
- **-batch**

  特記事項を表示しません。
- **-silent**

  操作中に何も表示しません
- **-nolimit**

  すべてのイベント・ビューアーを収集します。デフォルトは直前の 500 エントリーです。
- **-local**

  ローカル XML ファイルを作成します。
- **-listprobes**

  使用可能なプローブをリストします。
- **-probe**

  指定したプローブを実行します。

MAPDRV

MAPDRV は、ThinkVantage テクノロジー製品のネットワーク共有機能を提供します。 MAPDRV は、ThinkVantage テクノロジー製品とネットワーク共有の接続および切断に使用されます。ネットワーク共有情報はレジストリーに入っており、暗号

化されたストリングとしてネットワーク共用名を含んでいます。ネットワーク共有情報は、HKLM¥Software¥Lenovo¥MND¥<app id> のレジストリーに保管されています。

Active Directory ポリシーが使用される場合、これらの値は HKLM¥Software¥Policies¥Lenovo¥MND¥<app id> に保管されます。

MAPDRV を使用すると、暗号化エンジンを使用して暗号化されたユーザー名とパスワードを生成することができ、これらを使用して複数システムでネットワーク共有情報を定義できます。暗号化エンジンの使用によって、実行されているシステムのレジストリーが更新されることはありません。

MAPDRV へのコマンドライン・インターフェースは次のとおりです。

mapdrv /<function><app id> /unc <sharename> /user <username> /pwd <password> [/timeout <seconds>] [/s]

MAPDRV コマンドは、ネットワーク・ドライブを割り当てるためのユーザー・インターフェースを実行します。 mapdrv.exe コマンドは、C:¥Program Files¥Common Files¥Lenovo¥MND ディレクトリーにあります。ネットワーク・ドライブの割り当てのインターフェースは、以下のパラメーターをサポートします。

構文:

```
mapdrv [switches]
```

パラメーターを指定せずにコマンドを入力するとアプリケーションが起動します。情報を手動で入力する必要があります。

すべてのパラメーターの戻りコードは次のとおりです。

- **0** = 成功
- **> 0** = 失敗

パラメーターを指定せずに MAPDRV を起動すると、ネットワーク共有、ユーザー名、およびパスワードのプロンプトが出されます。次に、指定されたクレデンシャルを使用して指定されたネットワーク共有に接続しようと試行します。

次の表に、MAPDRV のパラメーターに関する情報および各パラメーターの結果を示します。

表 57. MAPDRV パラメーター

パラメーター	結果
/view	ネットワーク共有の表示を許可します。
/pwd	この共有の暗号化パスワードを指定します。
/store	アプリケーション ID、共用名、ユーザー名、パスワード、およびタイムアウト値を保管します。
/s	サイレントに設定します。接続できるかどうかに関わらずユーザーにプロンプトを出さない。
/timeout	タイムアウト値を設定します。
/unc	保管されているネットワーク共有。

表 57. MAPDRV パラメーター (続き)

パラメーター	結果
/user	保管されている、この共有の暗号化されたユーザー名を設定します。
/NetPath	実際の接続パスを示す MAPDRV からの値の出力を設定します。

MAPDRV の使用

次の例は、MAPDRV を使用する手順を示しています。

ThinkVantage テクノロジー製品のネットワーク共有情報を保管する: この機能は、ネットワーク共有情報をレジストリーに保管して、主要な MAPDRV レジストリー・キーのサブキーをオフに定義します。次のコマンドは、レジストリーの Unc、User、および Pwd の値を設定します。

mapdrv /store <app id> /unc <sharename> /user <username> /pwd <password>

[/timeout <seconds>]

接続共有と ThinkVantage テクノロジー製品を接続する: 次のコマンドは、レジストリーの Unc、User、および Pwd の値を使用して、共有に接続します。

mapdrv /connect <app id> [/s]

ネットワーク共有と ThinkVantage テクノロジー製品を切断する: 次のコマンドは、指定された ThinkVantage テクノロジーのネットワーク共有を現在接続されている場合は切断します。

mapdrv /disconnect <app id>

暗号化されたユーザー名とパスワードを表示する: 次のコマンドは、レジストリー・キーに保管されているネットワーク共有情報を表示するために使用されます。

mapdrv /view <app id> /user <username> /pwd <password>

Rescue and Recovery ブート・マネージャーの制御 (BMGR32)

ブート・マネージャー・インターフェースのコマンド・ライン・インターフェースは BMGR32 です。これは、フォルダー C:¥Program Files¥Common Files¥Lenovo¥BMGR にあります。下表に、BMGR32 のスイッチとその結果を示します。

表 58. BMGR32 のパラメーター

パラメーター	結果
/B0	区画 0 から起動する (区画テーブルの順序に基づく)。
/B1	区画 1 から起動する。
/B2	区画 2 から起動する。
/B3	区画 3 から起動する。
/BS	サービス区画から起動する。
/BW	Rescue and Recovery の隠し区画から起動する。

表 58. BMGR32 のパラメーター (続き)

パラメーター	結果
/BWIN	ワークスペースから起動するための要求をリセットする。これは、起動する前に呼び出す必要があります。
/CFG*file*	設定ファイル・パラメーターを適用する。設定ファイルに関する詳細については、 194 ページの『RRCMD コマンド・ライン・インターフェース』を参照してください。
/DS	マスター・ブート・レコード (MBR) データ・セクターを戻す (0 ベース)。
/D*n*	変更をディスク n に適用する。ここで n は 0 ベースです (デフォルト: 環境変数「SystemDrive」または、「SystemDrive」が見つからない場合は「C:¥」を含むディスク)。
/H0	区画 0 を隠す。
/H1	区画 1 を隠す。
/H2	区画 2 を隠す。
/H3	区画 3 を隠す。
/HS	サービス区画を隠す。
/P12	区画タイプを 12 に設定してサービス区画を隠す。
/INFO	ハードディスク情報を表示する (8 つのフリー・セクターを検査します)。
/INFOP	ハードディスク情報を表示する (16 のフリー・セクターを検査します)。
/M0	Rescue and Recovery ワークスペースはサービス区画にある。
/M1	Rescue and Recovery ワークスペースは C:¥PARTITION (Windows と Rescue and Recovery ワークスペースのデュアル・ブート)。
/M2	Rescue and Recovery ワークスペースは DOS のあるサービス区画にある (Rescue and Recovery ワークスペースと DOS のデュアル・ブート、Lenovo 製または IBM 製のプリロードのみ)。
/OEM	IBM 製または Lenovo 製 PC ではない。これにより、POST の後に強制的に F11 (デフォルト) キーを押す 2 回目のチェックが行われます。これは、IBM の古い PC で必要になる場合があります。
/Patch*n*	マスター・ブート・レコードのパッチ・プログラムがアクセスできる変数を設定するためにのみインストール・プログラムに使用されます。
Patchfile*filename*	マスター・ブート・レコードのパッチをインストールするためにのみインストール・プログラムに使用されます。
/PRTC	パッチ戻りコードを検索するために、インストール・プログラムのみに使用されます。
/IBM	IBM 製または Lenovo 製 PC である。
/Q	サイレント。
/V	冗長。
/R	PC を再起動する。

表 58. *BMGR32 のパラメーター (続き)*

パラメーター	結果
/REFRESH	データ・セクターの区画テーブル・エントリーをリセットする。
/THINK	キーボード上の青色のボタンを使用してワークスペースに入るようブート・マネージャーを構成する。
/TOC *tocvalue*	BIOS TOC ロケーションを設定する (8 バイトのデータを表す 16 文字)。
/U0	区画 0 を表示する。
/U1	区画 1 を表示する。
/U2	区画 2 を表示する。
/U3	区画 3 を表示する。
/US	サービス区画を表示する。
/F*mbr*	Rescue and Recovery ワークスペース (RRE) マスター・ブート・レコード・プログラムをロードする。
/U	Rescue and Recovery ワークスペース (RRE) マスター・ブート・レコード・プログラムをアンロードする。
/UF	マスター・ブート・レコード・プログラムを強制インストールまたはアンインストールする
/?	コマンド・ライン・オプションをリストする

/info 属性で bmgr.exe を起動する場合は、次の情報がダンプされます。

- **追加のマスター・ブート・レコード**

  最初のセクター以外の、マスター・ブート・レコードを含むセクター番号。

- **データ**

  マスター・ブート・レコードによって使用されるデータ・セクターのセクター番号。

- **パッチ・インデックス**

  マスター・ブート・レコードを使用して適用される任意のパッチのセクター番号。

- **Checksum return**

  チェックサム・エラーがない場合はこれは 0 でなければなりません。

- **起動区画**

  サービス区画の 1 をデフォルトとする区画テーブル・インデックス。

- **Alt 区画**

  存在する場合は、DOS 起動可能領域を示す区画テーブル・インデックス。

- **オリジナル MBR**

  PC のオリジナル・マスター・ブート・レコードが保管されているセクター番号。

- **IBM フラグ**

  データ・セクターの値 (IBM 製または Lenovo 製 PC の場合は 1、それ以外の場合は 0)

- **Boot Config**

  PC のレイアウトを説明する際に使用されるインストール・オプションを表示します。サービス区画が使用されたか、仮想区画が使用されたかを示します。

- **署名**

  データ・セクターおよび最初のセクターにある署名の値。「NP」が含まれていなければなりません。

- **休止期間**

  F11 メッセージが画面に表示される際の待ち時間の秒数 ¼ を表示します。

- **スキャン・コード**

  サービス区画を起動する場合に使用するキー。F11 キーのスキャン・コードは 85 です。

- **RR**

  BMGR では使用しません。Rescue and Recovery で設定します。

- **Prev Active Part**

  サービス区画から起動される場合に、前のアクティブ区画の区画テーブル・インデックスを表示します。

- **起動状態**

  PC の現在の状況を判別します。

  – 0 - オペレーティング・システムから通常どおり起動する。
  – 1 - サービス・オペレーティング・システムから起動する。
  – 2 - サービス・オペレーティング・システムから標準オペレーティング・システムに戻って起動する。

- **Alt ブート・フラグ**

  代替オペレーティング・システム、たとえば DOS から起動する。

- **前の区画タイプ**

  サービス区画から起動される場合、起動する前にサービス区画が設定された区画タイプを表示します。

- **前の IBM MBR Index**

  インストーラーが使用します。

- **Patch IN: OUT**

  パッチ・コードを使用する場合、このコードの入力値と出力値。

- **F11 Msg**

正しい BIOS 呼び出しがサポートされていないことをユーザーに表示するメッセージ。

次の表に、BMGR32 のエラー・コードおよびエラーの説明を示します。

表 59. BMGR32 エラー・コード

エラー・コード	エラーの説明
5	選択したオプションをマスター・ブート・レコードに適用しているときにエラーが発生しました。
6	マスター・ブート・レコードのインストール中にエラーが発生しました。
7	マスター・ブート・レコードのアンインストール中にエラーが発生しました。
10	システム・タイプを設定しているときにエラーが発生しました。
11	マスター・ブート・レコード・モードを設定しているときにエラーが発生しました。
13	互換性パッチのインストール中にエラーが発生しました。
14	互換性パッチ・パラメーターを設定しているときにエラーが発生しました。
96	セクターにアクセスしているときにエラーが発生しました。
97	セクターにアクセスしているときにエラーが発生しました。

RELOADSCHED

このコマンドは、レジストリーで定義されているスケジュール設定を再ロードします。レジストリーにスケジュールの変更を加える場合、変更をアクティブにするために、このコマンドを実行する必要があります。

例:

```
C:¥Program Files¥Lenovo¥Rescue and Recovery¥reloadsched
```

RRCMD コマンド・ライン・インターフェース

基本の Rescue and Recovery コマンド・ライン・インターフェースは RRCMD です。このコマンドは C:¥Program Files¥Lenovo¥Rescue and Recovery¥ サブディレクトリーにあります。次の表に、Rescue and Recovery のコマンドライン・インターフェースを使用するための情報が記載されています。

構文:

RRcmd *command filter=filterfile location=c* [name=*abc* | level=*x*] [silent]

表 60. RRcmd パラメーター

コマンド	結果
`Backup`	通常のバックアップ操作を開始する (場所および名前のパラメーターを含める必要がある)。
`Restore`	通常の復元操作を開始する (場所とレベルを含める必要がある)。
`List`	バックアップ・レベルに含まれるファイルをリストする (場所とレベルを含める必要がある)。

表 60. RRcmd パラメーター (続き)

コマンド	結果
Basebackup	代替基本バックアップを行う。これは増分バックアップの基礎として使用することができず、場所、名前、およびレベルを含める必要がある。レベルは 99 より大きくする必要がある。同じレベルを持つ別の基本バックアップがすでに存在する場合、それは上書きされる。
Sysprepbackup	PC が再起動した後、Rescue and Recovery ワークスペースでバックアップ操作を行う。この機能の主な用途は、Sysprep のバックアップを取り込むことです。 **注:** 1. 場合によっては進行状況表示バーが移動しないことがあります。この場合、ハードディスクを listen してバックアップを行っているかどうかを確認することができます。バックアップが終了している場合は、バックアップが終了しているというメッセージを受け取ります。 2. ネットワークに対する Sysprep バックアップを作成するときにパスワードを指定すると、増分バックアップが行われるまでパスワード・ファイルはバックアップ・ロケーションに書き込まれません。次の情報は、2 つの代替方法を示しています。 a. ローカル Sysprep のバックアップを作成して、ネットワークか USB にバックアップをコピーする。 b. Sysprep のバックアップ後にネットワークまたは USB に増分バックアップを作成し、その増分バックアップを維持するか削除する。
Copy	バックアップをある場所から別の場所にコピーする。このコマンドはアーカイブとも呼ばれ、これには場所を含める必要があります。
Rejuvenate	指定したバックアップにオペレーティング・システムを復元する。
Delete	バックアップを削除する。このコマンドには場所を含める必要があります。
Changebase	file.txt の内容に基づいて、すべてのバックアップ内のファイルを変更する。 file.txt 内のオプションは次のとおりです。 **A** 追加 **D** 削除 **R** 置換
Migrate	バックアップから移行ファイルを作成する。
Filter=*filterfile*	復元されるファイルおよびフォルダー。このコマンドは、**Restore** コマンドのみと併用されます。

表 60. RRcmd パラメーター (続き)

コマンド	結果
`Location=c`	以下のいずれか 1 つ以上を選択することができる。 **L** は内蔵ハードディスク・ドライブ **U** は USB ハードディスク **S** はセカンド・ハードディスク・ドライブ **N** はネットワーク **C** は CD/DVD 復元
`name=abc`	ここで *abc* はバックアップの名前です。
`level=x`	ここで *x* は 0 (基本) から増分バックアップの最大数 (復元オプションでのみ使用される) までの数値。バックアップ・コマンドでは、 100 以上の level=*x* という数値は管理者バックアップでのみ必要とされます。 **注:** 1. 最新のバックアップから復元するには、このパラメーターを使用しないでください。 2. すべてのバックアップおよび復元は、適切な順序を維持したりコールバックを実行するなどのために、サービスを介して実行されます。サービスに送られるバックアップ・コマンドは、コマンド・ライン・オプションによって置換されます。
ブート・マネージャー設定ファイル・フォーマット	ブート・マネージャー設定ファイルのフォーマットは、以前のバージョンのブート・マネージャーと後方互換です。下記に示されていないスイッチはサポートされていません。ファイル・フォーマットはテキスト・ファイルで、各項目は別の行にあります。 `<PROMPT1=this is the text that will appear on F11 prompt>` `<KEY1=F11>` `<WAIT=40>`
Osfilter	このコマンドは restore コマンドのみと併用されます。復元されるファイルをフィルタリングするために OsAppsList のレジストリー設定が使用されます。このコマンド・ライン項目は、OsApps 復元を実行するために使用できます。

基本バックアップのファイルを置換する方法

バックアップ内のファイルを置換するには、次のようにします。

1. バックアップにあるファイル (複数可) を変更します。たとえば、c:¥install.log です。
2. c:¥ のルートに file.txt というファイルを作成します。
3. file.txt を編集して、変更したファイルについてパス R=<変更したファイルへの絶対パス> を追加します。次に例を示します。

   ```
   R=c:¥install.log
   ```

   注: この file.txt を閉じる必要があります。
4. RRCMD Changebase filename=c:¥file.txt drive=c: destination=″c:¥RRBACKUPS″ を実行します

注: ユーザー・インターフェースで個別ファイルの復元を確認して、サイズの変更を通知します。

System Migration Assistant

このモジュールは以前の SMA4.2 smabat.exe と互換性があるコマンド・ライン・プログラムです。モジュールに対するコマンド・パラメーターおよび制御コマンドファイル (commands.txt) は SMA 5.1 と互換性がなければなりません。

System Update

System Update はローカル・システム上の更新クライアント PC を使用して、ユーザーとの対話を行わずに Web 上の希望するパッケージを配信します。System Update は更新されたクライアント PC を照会し、使用可能な更新クライアント PC を使用して希望するパッケージをインストールします。 System Update は ThinkVantage システム更新か、システム上のソフトウェア・インストーラーを起動します。

System Update Launcher がインストール済みかどうかを判別するには、次のレジストリー・キーの存在を確認します。

```
HKLM¥Software¥TVT¥ActiveUpdate
```

System Update を許可するようにレジストリーを構成するかどうかを決定するには、ThinkVantage テクノロジー・プログラムは EnableActiveUpdate 属性の値の独自のレジストリー・キーを検査する必要があります。EnableActiveUpdate=1 の場合、ThinkVantage テクノロジー・プログラムは「ヘルプ」メニューの下に「System Update」メニュー項目を追加する必要があります。

System Update を呼び出すには、呼び出し側 ThinkVantage テクノロジー・プログラムが System Update ランチャー・プログラムを起動して、パラメーター・ファイルを渡す必要があります。(パラメーター・ファイルの説明については、「System Update パラメーター・ファイル」を参照してください。)

すべての ThinkVantage テクノロジー・プログラムのヘルプ・メニューから System Update Launcher のメニュー項目を無効にするには、次の手順に従います。

1. HKLM¥Software¥ThinkVantage¥ActiveUpdate レジストリー・キーに進む。
2. ActiveUpdate キーの名前を変更するか削除する。

個々の ThinkVantage テクノロジー・プログラムのヘルプ・メニューから System Update Launcher のメニュー項目を無効にするには、次の手順に従います。

1. 次のレジストリー・キーに進む。
   - Rescue and Recovery の場合 - HKLM¥Software¥Lenovo¥Rescue and Recovery
   - Client Security Solution の場合 - HKLM¥Software¥Lenovo¥Client Security Software
2. DWORD 値 *EnableActiveUpdate* を追加して値を 0 に設定する。

個々の TVT のヘルプ・メニューの下で System Update Launcher メニュー項目が使用できない場合に、ヘルプ・メニューからこのメニュー項目を有効にするには、次の手順に従います。

1. 次のレジストリー・キーに進む。
   - Rescue and Recovery の場合 - HKLM¥Software¥Lenovo¥Rescue and Recovery
   - Client Security Solution の場合 - HKLM¥Software¥Lenovo¥Client Security Software
2. DWORD 値 *EnableActiveUpdate* を追加して値を 1 に設定する。

System Update パラメーター・ファイル

System Update パラメーター・ファイルには、System Update に渡される設定が含まれています。次の例で示すように TargetApp パラメーターが渡されます。

```
<root>
       <TargetApp>ACCESSLENOVO</TargetApp>
</root>
```

```
<root>
       <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>
</root>
```

付録 D. 管理者ツール

ThinkVantage テクノロジーは、企業の IT 管理者向けのツールを提供します。これらのツールは、Lenovo Web サイト
http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN
(英語のサイトです) からダウンロードできます。

Antidote ウィザード

Antidote ウィザードについて詳しくは、 207 ページの『付録 F. Antidote Delivery Manager コマンドの解説および例』を参照してください。

BMGR CLEAN

CleanMBR はマスター・ブート・レコードをクリーンアップします。このプログラムは、ブート・マネージャーのインストールに必要なセクターに十分な空きがないために Rescue and Recovery をインストールできないなどの、Rescue and Recovery インストール失敗が起こった場合に使用できます。

注:

1. このツールを実行すると、MBR を使用しているアプリケーションは使用できなくなります。たとえば、SafeGuard Easy、SafeBoot、および Computrace の MBR 版があります。
2. Rescue and Recovery をインストールする前に実行します。
3. DOS の場合は cleanmbr.exe を使用し、Windows の場合は cleanmbr32.exe を使用します。
4. DOS CleanMBR を実行した後で、FDISK /MBR を実行します。これは、MBR に置かれます。

cleanmbr32.exe のパラメーターは次のとおりです。

表 61.

パラメーター (必須)	**説明**
/A	MBR をクリアし、PC DOS MBR をインストールする
パラメーター (オプション)	
/Dn	ドライブへの変更を適用する。最初のドライブには `n=0` を使用してください。
/Y	すべて Yes
/?	ヘルプを表示する
/H	ヘルプを表示する

CLEANDRV.EXE

cleandrv.exe ファイルは、すべてのファイルのドライブをクリーンアップします。このコマンドを実行した後には、オペレーティング・システムはありません。詳しくは、 138 ページの『デプロイメント・シナリオ 5』を参照してください。

CONVDATE

CONVDATE ユーティリティーは、Rescue and Recovery 管理ツールの一部として提供されます。このユーティリティーは日付と時間の 16 進値を決定し、日付と時刻の値を 16 進値に変換するのに使用し、またカスタム日付と時間をレジストリーのバックアップ・フィールドに設定するのに使用することができます。

```
[Backup0]
StartTimeLow=0xD5D53A20
StartTimeHigh=0x01C51F46
```

CONVDATE ユーティリティーを実行するには、次のステップを実行します。

1. http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN (英語のサイトです) から Rescue and Recovery 管理ツールを抽出する。
2. CMD ウィンドウを開く
3. Convdate に入力する
4. DWORD 値を変換するには、日付と時間を選択するフィールドに日付と時間を入力する。

   注: 対応するレジストリー・ファイルの値は次のとおりです。

   - High DWORD=StartTimeHigh
   - Low DWORD=StartTimeLow

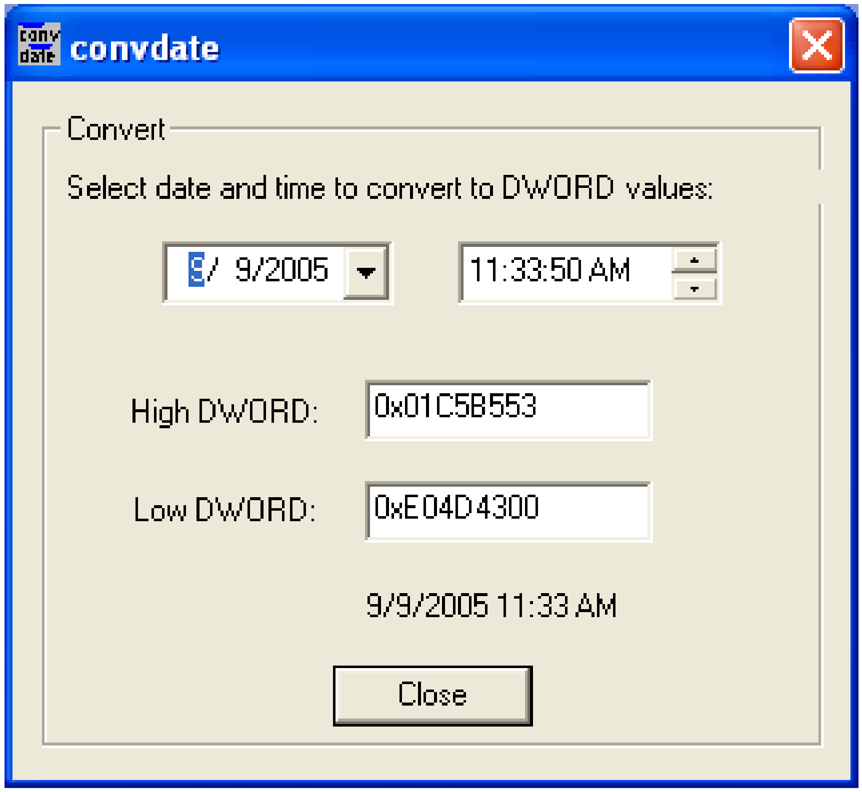


図 5. Convdate ウィンドウ

CREAT SP™

このコマンドは、希望するメガバイトでサービス区画を作成します。ドライブ名はオプションです。

構文は次のとおりです。

```
createsp size=x drive=x /y
```

CREAT SP のパラメーターは次のとおりです。

表 62.

パラメーター	説明
size=*x*	作成するサービス区画のサイズ (メガバイト)
drive=*x*	サービス区画を作成するドライブのドライブ番号。指定しない場合は、最初の非 USB ドライブが使用されます。このパラメーターはオプションです。
/y	クリーンアップされるドライブの確認をしない。このパラメーターはオプションです。

注: bmgr32.exe ファイルは、createsp.exe ファイルと同じフォルダーにあり、WinPE から実行する必要があります。

RRUTIL.EXE

rrutil.exe について詳しくは、 19 ページの『ワークスペース (Predesktop Area)』を参照してください。

SP.PQI

このファイルはタイプ 12 のサービス区画の作成に使用できます。詳しくは、 138 ページの『デプロイメント・シナリオ 5』を参照してください。

付録 E. ユーザーの作業

ユーザー権限の種類によって実行できない機能があります。次の表に、制限ユーザー、パワー・ユーザー、および管理者ユーザー (オペレーティング・システムがデフォルトで割り当てます) の基本的な操作機能の概要を示します。この機能は、Windows オペレーティング・システムによって若干、異なります。

Windows XP

次の表は、制限ユーザー、パワー・ユーザー、管理者ユーザーが Windows XP 環境の Rescue and Recovery で実行できる作業を示しています。

表 63. Windows XP のユーザー・タスク

Windows XP ユーザーが実行できる作業	**制限ユーザー**	**パワー・ユーザー**	**管理者**
レスキュー・メディア ISO を作成する。	いいえ	いいえ	はい (後述のコマンド・ラインを使用して)
起動可能 CD メディアを作成する。	はい	はい	はい
USB ハードディスク・ドライブ起動可能メディアを作成する。	いいえ	いいえ	はい
バックアップを開始する。	はい	はい	はい
Rescue and Recovery ワークスペース (RRE) で復元を開始する。	はい	はい	はい
Rescue and Recovery ワークスペースで個別ファイルの復元を行う。	いいえ (Windows) はい (Windows Pre Boot Area)	いいえ (Windows) はい (Windows Pre Boot Area)	はい
Rescue and Recovery インターフェースで包含および除外を設定する。	はい	はい	はい
ネットワーク・ドライブにバックアップする。	はい	はい	はい
バックアップのスケジュールを設定する。	はい	はい	はい

表 63. Windows XP のユーザー・タスク (続き)

Windows XP ユーザーが実行できる作業	制限ユーザー	パワー・ユーザー	管理者
Rescue and Recovery ワークスペース・ログイン ID の繰り上がり **注:** 最後の Windows 管理者 ID が、Windows から Rescue and Recovery ワークスペースに自動的に繰り上げられる唯一の ID です。Windows の制限ユーザーおよびパワー・ユーザーは、Rescue and Recovery ワークスペースにログオンするために自分のユーザー ID およびパスワードを再入力する必要があります。	いいえ	いいえ	はい

Windows 2000

次の表は、制限ユーザー、パワー・ユーザー、管理者ユーザーが Windows 2000 環境の Rescue and Recovery で実行できる作業を示しています。

表 64. Windows 2000 のユーザー・タスク

Windows 2000 ユーザーが実行できる作業	制限ユーザー	パワー・ユーザー	管理者
レスキュー・メディア ISO を作成する。	いいえ	いいえ	はい (後述のコマンド・ラインを使用して)
起動可能 CD メディアを作成する。	はい	はい	はい
USB ハードディスク・ドライブ起動可能メディアを作成する。	いいえ	いいえ	はい
バックアップを開始する。	はい	はい	はい
Rescue and Recovery ワークスペース (RRE) で復元を開始する。	はい	はい	はい
Rescue and Recovery ワークスペース (RRE) で個別ファイルの復元を行う。	いいえ (Windows) はい (Windows Pre Boot Area)	いいえ	はい
Rescue and Recovery インターフェースで包含および除外を設定する。	はい	はい	はい
ネットワーク・ドライブにバックアップする。	いいえ	いいえ	はい
バックアップのスケジュールを設定する。	はい	はい	はい

レスキュー・メディアの作成

管理者は、次のコマンド・ラインを使用してレスキュー・メディア ISO を作成できます。これらのコマンド・ラインを実行すると、ISO ファイルを作成することができ、ファイルは自動的に C:¥Program Files¥Lenovo¥Rescue and Recovery¥rrcd¥ フォルダーに置かれます。

```
:: This line will create the ISO silently and not burn it
```

```
C:¥Program Files¥Lenovo¥Common¥Python24¥python" "C:¥Program Files¥Lenovo¥Common¥spi
¥mkspiim.pyc /scripted
```

```
 /scripted
```

```
:: This line will create the ISO with user interaction and not burn it
```

```
C:¥Program Files¥Lenovo¥Common¥Python24¥python C:¥Program Files¥Lenovo¥Common¥spi
¥mkspiim.pyc /noburn
```

```
 /noburn
```

付録 F. Antidote Delivery Manager コマンドの解説および例

このセクションには、Antidote Delivery Manager のコマンドの解説および例が記載されています。Antidote Delivery Manager について詳しくは、 107 ページの『第 7 章 Antidote Delivery Manager のインフラストラクチャー』を参照してください。

Antidote Delivery Manager コマンドのガイド

ブート・マネージャーのコマンドライン・インターフェースは Antidote Delivery Manager です。これは、フォルダー C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM にあります。下表に、Antidote Delivery Manager のスイッチとその結果を示します。

表 65. Antidote Delivery Manager コマンド

コマンド	説明
`APKGMES [/KEY keyfile|/NEWKEY keyfile|/NOSIG] message_directory message_name [/NODATE]`	/KEY パラメーターが使用される場合、署名キーは keyfile.prv から取得され、keyfile.pub にあるキーは、メッセージを処理するすべてのクライアント PC に配布されていなければなりません。デフォルトでは、キー・ファイルには「KEYFILE.PRV」が使用されます。/NEWKEY パラメーターを使用してキーを作成することができます。署名が要求されない場合、/NOSIG を指定すると署名をしないことができます。メッセージ名の末尾に、*message_name*YYMMDDHHmm.zap のように日付スタンプが付加されます。
`REBOOT [/RR|/Win] [/wait | /f]`	このコマンドは PC を再起動します。パラメーターが指定されていない場合は、通常の起動シーケンスで再起動します。パラメーター RR は、再起動して Rescue and Recovery に入ることを意味し、WIN は再起動して通常のオペレーティング・システムに入ることを意味します。再起動はスクリプトを終了するまで発生しないので、これは通常スクリプト内の最後のコマンドであるはずです。オプションの WAIT コマンドは、PC に次回の再起動 (手動または他のメカニズムによって発生) 時に指定された環境に入るように強制します。/f パラメーターは、PC にすぐに再起動するよう強制し、開いているアプリケーションのデータをユーザーが保存するのを許可しません。パラメーターが指定されていない場合、プログラムはデフォルトで /win に入ります (/wait および /f が指定されていないものとみなします)。
`RETRYONERROR [ON|OFF] retries`	デフォルトで、スクリプトは 1 回のみ試行されます。ただし、スクリプトが正常に働くまでスクリプトを試行しつづけるのが重要な場合、RETRYONERROR コマンドを使用して、再試行パラメーターによって指定された有限の回数だけこのスクリプトの実行を試行し続けるよう通知することができます。回数が指定されない場合、デフォルト値は 3 です。

表 65. *Antidote Delivery Manager コマンド (続き)*

コマンド	説明
MSGBOX /msg *message text* [/head *header_text*] [/OK] [/CANCEL]│ [/TIMER *timeout*]	MSGBOX コマンドは、エンド・ユーザーがログオンされている場合は、このユーザーにメッセージを表示します。メッセージは表示されたままになり、タイムアウトが発生するか、「取消」ボタンが押されるか、「**OK**」ボタンが押される (/OK が指定されている場合) までスクリプトはブロックされます。/CANCEL が指定されていない場合、「取消」ボタンはパネル上に表示されず、キャンセルするのは非常に難しくなります。コマンドは次のコードを返します。 • 0 = OK が押された • 1 = CANCEL • 2 = タイマーが時間切れ メッセージにあるテキストは、改行およびタブを表すためにそれぞれ ¥n および ¥t を使用してフォーマット設定できます。
NETWK [/D│/E│/A [/IP *ip_address* │ /DN *domain_name*] [/NM *netmask*]	NETWK /D (無効) は、すべてのネットワーク・アダプターを無効にして、すべてのネットワーク・トラフィックを停止します。ネットワークは、NETWK /E (有効) コマンドが実行されるまで無効になります。NETWK /A は、ネットワークを IP アドレスに制限します。IP アドレスは /IP スイッチ (ドット「.」付き 10 進数) または /DN (DNS 名) によって指定されます。/NM スイッチはネットワーク・マスクを提供します。/NM が提供されていない場合は、/IP または /DN によって指定された単一 PC のみがアクセス可能になります。このコマンドの状態は再起動されても存続するので、ネットワークは明示的に有効にする必要があります。
APUBKEY [/ADD│/DEL] *asn_1_encoded_public_key*	APUBKEY コマンドにより、管理者は各 PC の Antidote Delivery Manager メッセージの署名キーをリモートから管理することができます。各 PC には、複数のキーを格納できます。署名されたメッセージが処理される場合、成功するキーが見付かるまで各キーが試行されます。キーは個別に名前が付けられていないので、内容によって参照する必要があります。新規のキーは ADD パラメーターを使用して追加し、DEL パラメーターを使用して削除することができます。
AUNCPW [/ADD│/CHANGE│/DEL] *unc* [/USER *userid*] [/PWD *password*] [/REF *ref_name*]	このコマンドにより、ネットワーク・ドライブ用のパスワードを追加、変更、または削除することができます。UNC を使用する代わりに、参照名をメッセージ内のショートカットとして使用することができます。戻り値は次のとおりです。 • 0 = 成功。 • 1 = 提供された情報を使用して設定できない。 • 2 = 成功、ただし同じ参照名を持つ別の UNC がすでに定義済み。

表 65. *Antidote Delivery Manager* コマンド (続き)

コマンド	説明
`XMLtool for Conditionals`	条件付き (eGatherer、現在のハードウェア情報) • **使用法:** xmltool.exe *filename xpath function comparator value* – **filename** XML ファイルへのパスおよびファイル名 – **xpath** 値への完全修飾 xpath – **function** 次の値のいずれかである必要があります。 - /C、値を比較する (comparator および value も提供する必要がある) - /v、指定された値を %SWSHARE%¥RET.TXT に書き込む – **Comparator:** 以下のいずれかである必要があります。 - LSS - LEQ - EQU - GTR - GEQ - NEQ – **Value:** XML 項目がこの値と比較されます。 • 戻り値: – **0** 比較により真と評価されました (/c) – **1** 比較により偽と評価されました – **2** 誤ったコマンド・ライン・パラメーター – **3** XML ファイルを開く際のエラー (存在しないか、ファイルにエラーがある) – **4** 指定された XPATH が値を戻しません • **例:** `xmltool.exe %swshare%¥¥lenovoegath.xml` `//system_summary/bios_version /C GEQ 1UET36WW`

表 65. Antidote Delivery Manager コマンド (続き)

コマンド	説明
INRR	INRR コマンドを使用してスクリプトが Rescue and Recovery ワークスペースで稼働中であるかどうか判別できます。戻り値は次のとおりです。 • 0 = 現行の OS が Win PE • 1 = 現行の OS が PE ではない • >1 = エラー
STATUS [/QUERY *location message_name* | /CLEAR *location]*	STATUS /QUERY コマンドを使用して、特定のメッセージがすでに実行されたか、実行されるのを待機しているか判別することができます。location の値は以下のいずれかである必要があります。 • **FAIL** メッセージがすでに実行され、失敗した • **SUCCESS** メッセージが正常に完了した • **WORK** メッセージが現在実行中か、Antidote Delivery Manager が次に実行されるときに実行される。 • **CACHE** メッセージが実行されるのを待機している。 STATUS/CLEAR コマンドは、指定された *location* をクリアします。戻り値は次のとおりです。 • 0 = 指定されたメッセージが検索されたか、コマンドが正常に完了した • 1 = 指定されたメッセージが検索されなかったか、コマンドが失敗した

表 65. *Antidote Delivery Manager* コマンド *(*続き*)*

コマンド	説明
MAILMAN [/RRU | RESET | /MB *mailbox* | /STATUS	このコマンドは、メールボックスの場所を検査して、そこで検出された修正を処理します。次のリストに、パラメーターを示します。 • **RRU** このパラメーターは、復元の後に毎回 Post Restore ディレクトリーにある .ZAP を実行します。 • **RESET** このパラメーターは、現在実行中のスクリプトの処理を停止します。 **注:** このパラメーターは、使用するとエラーの原因となる可能性があるため、状況を軽減するためだけに使用してください。 • **STATUS** このパラメーターは、Antidote プログラムの現行状態を示すためにビット・マスクを戻します。戻り値は次のとおりです。 – 0 = Antidote は正常に構成されている – 1 = 定義されたメールボックスがない – 2 = 定義された鍵がないか、NOSIG=1 が定義されていない

サポートされる Microsoft コマンド

次の表に、サポートされる Microsoft コマンドを示します。

表 66. サポートされる *Microsoft* コマンド

コマンド	説明
ATTRIB.EXE	ファイル属性を表示または変更する。
CACLS.EXE	ファイルのアクセス制御リスト (ACL) を表示または変更する。
CHKDSK.EXE	ディスクを検査し、状況報告を表示する。
COMP.EXE	2 つのファイルまたはファイルの集合の内容を比較する。
COMPACT.EXE	NTFS 区画上のファイルの圧縮を表示または変更する。
CONVERT.EXE	FAT ボリュームを NTFS に変換する。カレント・ドライブを変換することはできません。
DISKPART.EXE	ドライブを区画化する。
FC.EXE	2 つのファイルまたはファイルの集合を比較し、それらの間の相違点を表示する。
FIND.EXE	ファイル内のテキスト文字列を検索する。
FINDSTR.EXE	ファイル内の文字列を検索する。
FORMAT.COM	ディスクを Windows で使用するようにフォーマット設定する。

表 66. サポートされる Microsoft コマンド (続き)

コマンド	説明
LABEL.EXE	変更を作成するか、ディスクのボリューム・ラベルを削除する。
NET.EXE	ネットワーク・コマンドを指定する。
PING.EXE	ネットワーク・リソースに到達できるか検査する。
RECOVER.EXE	不良または欠陥のあるディスクから読み出すことのできる情報を復元する。
REG.EXE	レジストリーの操作。
REPLACE.EXE	ファイルを置換する。
RRCMD.EXE	OS からバックアップを取るか、OS または Rescue and Recovery ワークスペースから復元を行う。
SORT.EXE	入力をソートする。
SUBST.EXE	パスをドライブ名と関連付ける。
XCOPY.EXE	ファイルおよびフォルダー・ツリーをコピーする。

準備およびインストール

以下の手順は、Antidote Delivery Manager および Rescue and Recovery の準備とインストールに関する情報を提供します。

準備

署名キーが使用される場合、新規の署名キーを生成するため、 /NEWKEY パラメーターを使用してパッケージ化ツールを実行します。

設定

いくつかの設定項目が必要となります。項目は rnrdeploy.xml ファイルにあります。

リポジトリー

各クライアント PC はリポジトリーのリストを必要とします。これは UNC で指定された少なくとも 1 つのネットワーク・ドライブに加え、ディスケットおよび C:¥ です。「mailbox =」は、メールボックスの場所へのドライブおよびパスをコンマを付け、重要な順に区切って含める必要があります。

例:

```
[rescue] mailbox = %y%¥antidote, c:¥antidote
```

スケジュール情報

スケジュール情報は、次の設定値を使用して、HKEY_LOCAL_MACHINE¥SOFTWARE¥Lenovo¥Scheduler¥Tasks¥Rescue and Recovery¥ のレジストリーに設定することができます。

- ″Task″=″C:¥¥Program Files¥¥Lenovo¥¥Rescue and Recovery¥¥rrcmd.exe″
- ″TaskParameters″=″BACKUP location=L name=¥″Scheduled¥″ scheduled″
- ″Mode″=dword:00000004 ″Hour″=dword:00000012

- ″Minute″=dword:00000000 ″DayOfWeek″=dword:00000003
- ″WakeFromSuspendHibernate″=dword:00000000

Schedule Mode は、確認を表します。

表 67. スケジュール・モード

スケジュール・モード	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080
SCHED_NETWORK_DETACH	0x100

署名キー

署名キーが使用される場合、それをクライアント PC に配布する必要があります。APKGMES コマンドによって作成されたファイル keyfile.pub にはキーが含まれます。許可された各公開署名キーはレジストリーに表示されます。APUBKEY 機能を使用して、この値を `nosig =` と設定します。これが 1 に設定される場合、未署名パッケージ (/NOSIG パラメーターを使用して作成されたパラメーター) を実行させることができます。

注: 1 に設定されないか、公開キーがレジストリーにある場合、未署名パッケージは実行されません。

ネットワーク・ドライブ

以下の値は、AUNCPW の機能により `RscDrvY` セクション内に設定され、HKLM¥Software¥Policies¥Lenovo¥MND¥4.0¥AD のレジストリーに保管されます。/NEWKEY パラメーターを使用してキーを作成することができます。署名が要求されない場合、/NOSIG を指定すると署名をしないことができます。各 `RscDrv` セクションには 1 つのネットワーク共有に関する情報が含まれます。最大 10 のネットワーク共有を Antidote Delivery Manager 用に定義できます。

- UNC = Antidote Delivery Manager が接続するべきドライブの UNC (汎用命名規則)。
- User = 暗号化されたユーザー名。
- Pwd = 暗号化されたパスワード。
- Ref = この接続に関連付けられる参照名。

クライアント PC でのインストール

Rescue and Recovery 3.1 は、すべてのクライアント PC にインストールされている必要があります。上記で準備した設定は、インストール時に行うことができますが、後で実行しても構いません。

サーバー・インフラストラクチャー

管理者は、リポジトリー用のネットワーク共有を設定するか、FTP または HTTP サイトを提供する必要があります。修正およびパッチ用に追加のリポジトリーが必要になる場合があります。

単純なシステムのテスト - 通知の表示

go.rrs スクリプトを Antidote Delivery Manager をインストール済みのいずれかの PC に書き込みます。`MSGBOX /MSG "Hello World" /OK` という行を含むようにします。コマンドをコマンド・プロンプトから実行し、それが望みどおり機能していることを確認します。次に、go.rrs を含むフォルダーで APKGMSG コマンドを実行して、メッセージを作成します。メッセージ・ファイルを PC のリポジトリー・フォルダーのいずれか 1 つに配置し、正しく動作するか監視します。

デプロイメント

Antidote Delivery Manager をデプロイする前に、次のステップを実行します。

1. メールボックスの位置を決定します。
   - メールボックス は、ネットワーク共有、ハードディスクのローカル・システムまたは取り外し可能メディア、または FTP、HTTP サイトでディレクトリーとして定義されます。
   - 複数のメールボックスを所有していると、1 つのメールボックスにアクセスできない場合に便利です。メールボックスの位置を最大 10 まで定義できます。
   - ネットワーク・ベースのメールボックスは、クライアント PC で読み取り専用とし、書き込みアクセスを制限します。
2. レジストリーでリポジトリーをセットアップします。
   - Rescue and Recovery をインストールしたドナー・システムで、HKLM¥Software¥Lenovo¥Rescue and Recovery¥3.1¥ADM のレジストリーを編集します。
   - 上記のキーで次の設定を変更します。

     ```
     mailbox=
     ```

     次にメールボックス・ディレクトリー情報を追加します。たとえばローカル・ドライブのメールボックスは次のようになります。

     ```
     [rescue]
     mailbox=C:¥ADM¥Mailbox,
     ¥¥Machine¥Share¥Directory
     ```

     FTP サイトのメールボックスは次のようになります。

     ```
     ftp://userid:password@ftpserver/mailbox
     ```

     共有回線網ドライブのメールボックスは次のようになります。

```
¥¥Machine¥Share¥Directory
```

注:

a. HTTPS は、メールボックス機能ではサポートされていません。

b. HTTP Web サーバーは索引付けをオンにし、ファイルをリストする機能を配信するように構成する必要があります。

ドライブ名は、Windows Professional Edition およびご使用の通常オペレーティング・システム環境の間で変更される場合があります。最も変更される可能性が高いのは C: ドライブです。これを回避するには、環境変数 *CUSTOS* を使用します。これは常に標準的カスタマー・オペレーティング・システムを含むドライブをポイントします。前述の例は次のように変更されます。

```
mailbox=%CUSTOS%¥ADM¥Mailbox,ftp://userid:password@ftpserver/mailbox,
 ¥¥Machine¥Share¥Director
```

ストリングは、使用する装置またはプロトコルの標準に準拠する限り、どのような長さにもできます。たとえば、ローカル・ファイルを使用している場合、パスは 256 文字を超えることはできません。

- 複数メールボックス項目は、コンマまたはセミコロンで分離されます。
- Antidote Delivery Manager はパッケージの指定されたメールボックスの位置を順番に調べます。

3. FTP または HTTP 接続にユーザー名およびパスワードが必要な場合、次のフォーマットを使用します。

```
ftp//username:password@ftp.yourmailbox.com
```

4. ユーザー名とパスワードに応じて、ネットワークはメールボックスを共有します。

ユーザー名とパスワードの項目は、暗号化されてレジストリーに保管されます。ドナー・システムに項目を追加するには、次を実行します。

a. DOS ウィンドウを開きます。

b. フォルダーを `C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM` に変更します。

c. 次のコマンドを実行します。

```
auncpw /add ¥¥Machine¥Share¥Director /user username /pwd password /ref refID
```

このコマンドではレジストリーに次の項目を作成します。

```
[RscDrv0]
UNC=¥¥Network¥Share
User=01E23397A54D949427D5AF69BF407D5C
Pwd=04E22197B34D95943ED5A169A0407C5C
Ref=refID
```

注:

a. この項目は、同じ共有へのアクセスを取得するため Antidote Delivery Manager によって使用されるあらゆるシステムで使用できます。

b. Antidote Delivery Manager は、最大 10 のネットワーク共有を使用できます。

c. 10 のネットワーク共有に加え、FTP または ローカルなど、その他のメールボックス項目を追加できます。

d. auncpw.exe ファイルには、この他にパスワード管理に使用できる機能があります。コマンド・ラインで AUNCPW /? を入力するか、 207 ページの表 65 を参照してください。

5. Antidote Delivery Manager 公開/秘密鍵ペアを作成します。セキュリティーを強化するために、Antidote Delivery Manager の公開/秘密鍵ペア機能を使用してください。Antidote Delivery Manager は、公開/秘密鍵ペアを使用してパッケージの認証性を検査します。秘密鍵は確実に保護し、配布しないようにします。一致する公開鍵は、 Antidote Delivery Manager で管理される各クライアント PC になくてはなりません。インストールされた Rescue and Recovery で非ドナー・システムに公開/秘密鍵ペアを作成するには、次を実行します。

   a. DOS ウィンドウを開きます。

   b. C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM に CD コマンドを発行します。

   c. 次のコマンドを実行します。

   ```
   apkgmes.exe /newkey mykey
   ```

   このコマンドは、mykey.pub および mykey.prv の 2 つのファイルを作成します。順に、公開鍵、秘密鍵です。

   d. ドナー・システムの C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM フォルダーに公開鍵をコピーします。

   e. notepad.exe などのテキスト編集プログラムを使用してファイルを開きます。

   f. クリップボードにファイルの内容をコピーします。

   g. コマンド・ラインに以下を入力します。

   ```
   apubkey.exe /add x
   ```

   ここで *x* はクリップボードの内容です。

   h. これにより、「レスキュー」セクションのレジストリーに項目が作成されます: pubkey0=906253...。

   - 最大 10 の公開鍵をレジストリーに保管できます。
   - apubkey.exe ファイルには、公開鍵管理に使用できる別の機能があります。コマンド・ラインで APUBKEY /? と入力するか、 207 ページの表 65 を参照します。

6. Schedule Antidote Delivery Manager チェックを作成します (複数のスケジュールを許可)。Antidote Delivery Manager はシステムで定期的に実行する必要があります。20 分ごとに実行するスケジュールをセットアップするには、ドナー・システムのレジストリーに以下を追加します。

   ```
   HKLM¥Software¥Lenovo¥Scheduler¥Rescue0
   Mode=1
   NumMinutes=20
   TaskShow=1
   Task=C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM¥antidote
   ¥mailman.exe
   ```

   注:

   a. スケジューラーは Rescue and Recovery ワークスペースで稼働しません。

   b. 詳しくは、 145 ページの『バックアップおよび関連タスクのスケジューリング』を参照してください。

7. Antidote Delivery Manager パッケージを作成します。

   ここまでのステップを完了したら、ご使用の最初のパッケージをビルドし、配布します。管理者システム (非ドナー) で、以下を実行します。

   a. *C:¥ADM¥Build* などのディレクトリーを作成します。
   b. そのディレクトリーで、go.rrs という名前のファイルを作成し、以下を追加します。

      ```
      msgbox.exe /msg "Hello World!" /head "test" /ok /cancel
      ```

   c. ファイルを保存してクローズします。
   d. C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM に CD コマンドを発行します
   e. 次のコマンドを実行します。

      ```
      apkgmes.exe /key mykey.prv C:¥adm¥build HELLOPKG
      ```

   f. これにより HELLOPKGYY*MMDDHHMM*.ZAP という名前のパッケージが作成されます。ここで *MMDDHHMM* は現在日時に置き換えられます。
8. HELLOPKGYY*MMDDHHMM*.ZAP をステップ 2 で指定したメールボックスの位置にコピーします。
9. Antidote Delivery Manager を実行します。
   a. ドナー・システムのタイマーが期限切れになると、パッケージが稼働し、「Hello World」メッセージ・ボックスが表示されます。
   b. 待ちたくない場合は、ドナー・システムで C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM¥mailman.exe を入力することができます

例

以下は、Antidote Delivery Manager の使用例です。

例 1

これは、レジストリーにあるウィルスまたは不正項目のため、常に青色の画面となっている PC を修正するパッケージの例です。

1. クライアント PC が青色の画面を表示している原因は、レジストリーの Run キーを通じて感染したウィルスによるものと仮定します。これを修正するには、*reg* を実行する、go.rrs という名のファイルを作成する必要があります。Microsoft コマンドのリストについては、 211 ページの『サポートされる Microsoft コマンド』を参照してください。可能であれば、*Reg* からレジストリー値を削除し、システムから実行可能ファイルを削除します。内容は次のようになります。

   ```
   reg delete HKLM¥Software¥Microsoft¥Windows¥Current Version¥Run /v runvirusvalue
   /f del %custos%¥windows¥system32¥virus.exe
   ```

2. ご使用の *C:¥ADM¥BUILD* ディレクトリーに go.rrs ファイルを置き、以下を実行します。

   ```
   apkgmes.exe /key mykey.prv C:¥ADM¥BUILD REMOVEVIRUS
   ```

3. ご使用のメールボックスに REMOVEVIRUS*YYDDHHMM*.ZAP をコピーします。
4. それぞれのクライアント PC を起動し、「ThinkVantage」ボタン、F11 または Enter キーを押して Rescue and Recovery ワークスペースに移動します。

例 2

この例では、Quick Fix Engineering 更新を強制するか、またはクライアント PC にパッチを当てます。

1. *C:¥ADM¥PATCHBUILD* のような、スクリプト・ファイルとパッチ・ファイルを保留するディレクトリーを作成します。
2. C:¥ADM¥PATCHBUILD ディレクトリーに qfe またはパッチ実行可能ファイルを置きます。
3. go.rrs という名のファイルを作成し、そこに次の行を置きます。ただし、Microsoft Quick Fix Engineering またはパッチを実行しインストールする行をカスタマイズします。 このパッチは通常の Windows オペレーティング・システムにしかインストールできないので、このスクリプトはインストールが Windows Professional Edition で実行されないようにします。

```
set custos
if errorlevel 1 set custos=%systemDrive%
%custos%¥Program Files¥Lenovo¥Rescue and Recovery¥ADM¥retryonerror
/on 10
%custos%¥Program Files¥Lenovo¥Rescue and Recovery¥ADM¥InRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto InPE

:ERROR
exit 1

:InOS
REM DISABLE NETWORKING
Netwk.exe /d
patchinstall.exe
REM ENABLE NETWORKING
Netwk.exe /e
msgbox.exe /msg "Patch Installed" /head "Done" /ok
exit 0

:InPE
exit 1
```

4. go.rrs を C:¥ADM¥PATCHBUILD ディレクトリーに置き、実行します。

```
apkgmes.exe /key mykey.prv C:¥ADM¥PATCHBUILD PATCHBUILD
```

5. ご使用のメールボックスに PATCHBUILD*YYDDHHMM*.ZAP をコピーします。
6. パッチは、クライアント PC の mailman.exe ファイルの次の実行時、またはクライアント PC の再起動時にインストールされます。

パッケージ完了ログ

- **Fail log**

  このファイルは通常 *C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM* ディレクトリーに保管されます。ゼロ以外の値を持つ .zap ファイルが終了する場合、このファイルにログされます。

- **Rescue.log**

  このファイルは通常 *C:¥SWSHARE* ディレクトリーに保管されます。このファイルは、パッケージが失敗した理由、またはパッケージを作動させる方法を判別するのに役立つ詳細情報を提供します。このファイルは、.zap ファイルでの現象を行ごとにロギングしています。

- **Success log**

  このファイルは通常 *C:¥Program Files¥Lenovo¥Rescue and Recovery¥ADM* ディレクトリーに保管されます。.zap ファイルがゼロの値で終了する場合、ここにログされます。

例 3

この例は Rescue and Recovery ワークスペースの FTP または HTTP サイトを使用します。

1. 以下のパッケージ用に、外部 Web サイトを定義する。
   ```
   ftp.yourmailbox.com
   ```
2. 公開および秘密鍵を作成する。ステップ 5 を参照してください。
3. レジストリーにメールボックスを追加します。
   ```
   mailbox=ftp://username:password@ftp.yourmailbox.com
   ```
4. Rescue and Recovery ワークスペースに入るため、ユーザーが F11 または Enter キーを押すと、起動時に Antidote Delivery Manager パッケージが Rescue and Recovery ワークスペースで実行します。

例 4

この例は、特定のクライアント PC をターゲットにした xmltool.exe ファイルを使用します。

1. アクティブ・ディレクトリー、Systems Management Server またはその他の管理ツールを通して、ご使用のクライアント PC と比較したい情報を含む XML ファイルを配布します。
   ```
   <file>
   <activedirgroup>Marketing</activedirgroup>
   </file>
   ```
2. go.rrs ファイルの最初の行に、XML ツールを使用する行を置きます。この行は、Marketing グループ内の PC をターゲットにするのみの例です。
   ```
   xmltool.exe c:¥mycompany¥target.xml //file/activedirgroup /c EQU Marketing
   if errorlevel 0 goto RUNIT
   exit errorlevel

   :RUNIT
   #place code to execute patch or whatever action
   ```

スクリプトの例

スクリプトの例については、

http://www.lenovo.com/pc/support/site.wss/document.do?lndocid=TVAN-ADMIN にある管理者ツール・パッケージをダウンロードしてください。

付録 G. 特記事項

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、レノボ・ジャパンの営業担当員にお尋ねください。本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、Lenovo 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

Intellectual Property Licensing
Lenovo Group Ltd.
3039 Cornwallis Road
Research Triangle Park, NC 27709
USA
Attention: Dennis McBride

Lenovo およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。 国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書におけるいかなる記述も、Lenovo あるいは第三者の知的所有権に基づく明示または黙示の使用許諾と補償を意味するものではありません。本書に記載されるすべての情報は、特定の環境において得られたものであり、例として提示されます。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

商標

以下は、Lenovo Corporation の商標です。

Lenovo
Rescue and Recovery
Client Security Solution
ThinkPad
ThinkCentre
ThinkVantage
Rapid Restore

Intel は Intel Corporation の米国およびその他の国における商標です。

以下は、IBM Corporation の商標です。

- IBM
- Lotus
- Lotus Notes

Microsoft、Windows、および Windows NT は、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

用語集

［ア行］

暗号化システム (Cryptography system). 暗号化システムは、データの暗号化と復号の両方を行う単一の鍵を使用する対称鍵暗号化と、2 つの鍵 (全員に知られている公開鍵と鍵ペアの所有者のみがアクセス権を持つ秘密鍵) を使用する公開鍵暗号化に、大きく分類される。

エンベデッド・セキュリティー・チップ. エンベデッド・セキュリティー・チップは、TPM の別名。

［カ行］

管理者 (ThinkCentre)/スーパーバイザー (ThinkPad) BIOS パスワード. 管理者パスワードまたはスーパーバイザー・パスワードは、BIOS 設定を変更する能力を制御するために使用される。これには、エンベデッド・セキュリティー・チップを使用可能または使用不可にして、TPM 内に保管されたストレージ・ルート鍵をクリアする機能が含まれる。

公開鍵/非対称鍵暗号化 (Public-key/Asymmetric-key encryption). 公開鍵アルゴリズムは通常、2 つの関連した鍵のペアを使用する。1 つは秘密に保持されなければならない秘密鍵で、もう一方は公開される鍵で広く配布される。鍵が 1 つあった場合、ペアのもう一方が推測できるようであってはならない。「公開鍵暗号化」という用語は、鍵の一部を公開情報にするというアイデアから得られる。すべてのパーティーが同じ情報を保持しないことから、非対称鍵暗号化という用語も使用される。ある意味では、1 つの鍵がロック (暗号) を「ロック」し、別の鍵はそれをアンロック (復号) することを要求される。

［サ行］

ストレージ・ルート鍵 (SRK). ストレージ・ルート鍵 (SRK) は 2,048 ビット (あるいはそれ以上) の公開鍵ペア。これは最初は空で、TPM 所有者が割り当てられたときに作成される。この鍵ペアは、エンベデッド・セキュリティー・チップをそのままでは放置しない。 TPM の外部にあるストレージの秘密鍵を暗号化 (ラップ) し、TPM にロード・バックされたときにそれらを復号する。 SRK は、BIOS にアクセスのある人なら誰でもクリアすることができる。

［タ行］

対称鍵暗号化 (Symmetric-key encryption). 対称鍵暗号化暗号はデータの暗号化と復号に同じ鍵を使用する。対称鍵暗号は簡単で高速だが、主な欠点は、2 つのパーティーが何らかのセキュアな方法で鍵を交換しなければならないことにある。公開鍵暗号化は、公開鍵は非セキュアな方法で配布可能であり、秘密鍵は転送されることがないので、この問題を回避している。 Advanced Encryption Standard は対称鍵の一例。

A

Advanced Encryption Standard (AES). *Advanced Encryption Standard* は*対称鍵*暗号化技法。アメリカ政府は、それまで使用していた DES 暗号化に置き換えて、このアルゴリズムをその暗号化技法として 2000 年 10 月に採用。 AES は、凶暴なアタックに対して 56 ビット DES キーよりも高度のセキュリティーを提供する。また AES では、必要に応じて 128、192 および 256 ビット・キーの使用が可能。

T

TPM (Trusted Platform Module). TPM は特別な目的を持ってシステム内にビルドされた集積回路で、強力なユーザー認証と PC 検査を可能にする。 TPM の主な目的は、機密情報への不適切なアクセスを防止することにある。 TPM はハードウェア・ベースの信頼の基幹機能で、システム上のさまざまな暗号サービスを提供するように活用することができる。 TPM の別名はエンベデッド・セキュリティー・チップ。

Printed in Japan